UNDERSTANDING THE CYBER THREAT AND IMPLICATIONS FOR THE 21ST CENTURY ECONOMY

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

MARCH 3, 2015

Serial No. 114–17

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
95–373 WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota

FRANK PALLONE, Jr., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DeGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY McNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJÁN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California

Subcommittee on Oversight and Investigations

TIM MURPHY, Pennsylvania
Chairman

DAVID B. McKINLEY, West Virginia
Vice Chairman
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
H. MORGAN GRIFFITH, Virginia
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

DIANA DeGETTE, Colorado
Ranking Member
JANICE D. SCHAKOWSKY, Illinois
KATHY CASTOR, Florida
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
JOSEPH P. KENNEDY, III, Massachusetts
GENE GREEN, Texas
PETER WELCH, Vermont
FRANK PALLONE, Jr., New Jersey *(ex officio)*

CONTENTS

WITNESSES

SUBMITTED MATERIAL

[1] Available at: *http://docs.house.gov/meetings/if/if02/20150303/103079/hhrg-114-if02–20150303-sd006.pdf.*

UNDERSTANDING THE CYBER THREAT AND IMPLICATIONS FOR THE 21ST CENTURY ECONOMY

TUESDAY, MARCH 3, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 2:30 p.m., in room 2322 of the Rayburn House Office Building, Hon. Tim Murphy (chairman of the subcommittee) presiding.

Members present: Representatives Murphy, McKinley, Burgess, Blackburn, Bucshon, Brooks, Mullin, Hudson, Collins, Cramer, DeGette, Clarke, Kennedy, Green, and Pallone (ex officio).

Staff present: Charlotte Baker, Deputy Communications Director; Leighton Brown, Press Assistant; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Brittany Havens, Legislative Clerk; Charles Ingebretson, Chief Counsel, Oversight and Investigations; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; John Ohly, Professional Staff, Oversight and Investigations; Chris Santini, Policy Coordinator, Oversight and Investigations; Peter Spencer, Professional Staff Member, Oversight; Jessica Wilkerson, Legislative Clerk; Christine Brennan, Democratic Press Secretary; Jeff Carroll, Democratic Staff Director; Chris Knauer, Democratic Oversight Staff Director; Una Lee, Democratic Chief Oversight Counsel; and Elizabeth Letter, Democratic Professional Staff Member.

OPENING STATEMENT OF HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. MURPHY. Well, good afternoon. I now convene this hearing of the Oversight and Investigations Subcommittee, entitled, "Understanding the Cyber Threat and Implications for the 21st Century Economy." This is the first in a series of hearings by this committee focused on cyberspace, the Internet, and the challenges and opportunities that they present for the 21st century economy.

These are big, important issues, so it is imperative that we establish a clear understanding of the issues we face. So today we are going to do something a little different. We are not here to examine a specific cybersecurity incident, policy issue, or legislative proposal. Today we are going to take a step back and explore some fundamental questions with our experts. Such things as what is the breadth and depth of the cyber threats? Is it something that can be solved? And what does this mean for the future?

In 1969, computers at four universities connected to the ARPANET, thus proving a computer networking concept that evolved into what we now know as the Internet. Since its inception, the Internet has been an open platform, designed to facilitate the transfer of data and information between remotely located computing resources. It doesn't discriminate against any network or device, nor the transmission of the data. It is merely a conduit for information. This open architecture, end-to-end system design is what makes the Internet such a benefit to society. It provides endless possibilities for innovation. It gives any individual with an Internet connection an opportunity to share their opinion with the world, and to access a nearly infinite amount of information. It has revolutionized the way we conduct business, interact socially, learn, and consume information, be it true or false. As a result, the Internet fostered widespread development and adoption of computing and communications technologies, collectively known as information technologies. Today, we depend on these technologies for everything from social interaction to home security, the operation of critical services like power plants and the electric grid. This integration of the Internet and information technologies into nearly every aspect of modern life has created the virtual world commonly known as cyberspace.

The Internet's strength, however, is also its weakness. It is by nature an open system with many interconnections, creating multiple opportunities for disruption. Likewise, information technologies are inherently complex systems, increasing the probability of ingrained vulnerabilities. As a result, the same technological and cultural factors that facilitate real-time global interaction, rapid innovation, and freedom of expression empower malicious actors to thrive and create risk in cyberspace.

The challenge arises from the fact that cyberspace creates an asymmetric imbalance that strongly favors malicious actors. Anyone, from an individual to a nation state, can target a victim halfway around the world at minimal cost and with little risk of being caught. Because the cost of failure and the consequences of crime are minimal, the threat evolves rapidly. In contrast, the costs of defense, as well as potential consequences, are significant. Because this asymmetric threat is rooted in the fundamental structure of the Internet and information technology, there is no way to solve cybersecurity without undermining the benefits of the cyberspace. There is no silver bullet or technological solution. While we certainly can do more toimprove the security of cyberspace, these decisions require a thoughtful cost benefit analysis. How will a potential security measure affect the cost or convenience of a product? How will it affect the pace of innovation? What will it mean for privacy or civil liberties? Cyberspace is no longer a place that we visit; it is the place where we live. Ten years ago, smartphones were a novelty, in fact, the iPhone didn't even exist. Today, mobile devices serve as a credit card, they can track our health, unlock our homes, start our vehicles, and document our daily travels. A pacifier can monitor your infant's temperature and send that information directly to your computer or mobile device. Through what is known as the Internet of things, we have connected kitchen appliances, you can start dinner from the office, check social media accounts from your grill, or know when you are low on milk.

Cyberspace is, and will increasingly be, the economic engine of the 21st century economy, and at the same time as the Internet and information technology become increasingly entwined in our daily routines, cyberspace becomes a limitless and adaptive attack surface. The security challenges will be more diverse and harder to predict, and the consequences will be more severe. We may not be able to secure cyberspace, but it is our collective responsibility to understand the threat in order to minimize its effect on our privacy, civil liberties, national security, and economic prosperity. We should embrace this unique opportunity this hearing presents, not to debate data breach legislation or other specific policy issues, but to listen.

We are privileged to have an impressive panel of experts who can help us understand the challenges of cybersecurity in context. In particular, I want to recognize Dr. Shannon from Carnegie Mellon University in Pittsburgh, home to the Nation's first computer emergency response team. The Pittsburgh region boasts some of the Nation's foremost experts in the field of cybersecurity, and I am pleased to have one of those experts, Dr. Shannon, joining us here today.

[The prepared statement of Mr. Murphy follows:]

PREPARED STATEMENT OF HON. TIM MURPHY

This is the first in a series of hearings by this Committee focused on cyberspace, the Internet and the challenges and opportunities that they present for the 21st century economy. These are big, important issues, so it is imperative that we establish a clear understanding of the issues we face.

So, today we are going to do something a little different. We are not here to examine a specific cybersecurity incident, policy issue or legislative proposal. Today, we are going to take a step back and explore some fundamental questions. Why does the cyber threat exist? Is it something that can be solved? And what does this mean for the future?

In 1969, computers at four universities connected to the ARPANET, thus proving a computer networking concept that evolved into what we now know as the Internet. Since its inception, the Internet has been an open platform, designed to facilitate the transfer of data and information between remotely located computing resources. It does not discriminate against any network or device, nor the data they transmit. It is merely a conduit for information.

This open architecture, end-to-end system design is what makes the Internet such a benefit to society. It provides endless possibilities for innovation. It gives any individual with an Internet connection an opportunity to share their opinion with the world. It has revolutionized the way we conduct business, interact socially, learn and consume information.

As a result, the Internet fostered widespread development and adoption of computing and communications technologies, collectively known as information technology. Today, we depend on these technologies for everything from social interaction to the operation of critical services like the electric grid. This integration of the Internet and information technologies into nearly every aspect of modern life has created the virtual world commonly known as cyberspace.

The Internet's strength, however, is also its weakness. It is by nature an open system with many interconnections, creating multiple opportunities for disruption. Likewise, information technologies are inherently complex systems, increasing the probability of ingrained vulnerabilities. As a result, the same technological and cultural factors that facilitate real-time global interaction, rapid innovation, and freedom of expression empower malicious actors to thrive and create risk in cyberspace.

The challenge arises from the fact that cyberspace creates an asymmetric imbalance that strongly favors malicious actors. The nature of the Internet and complexity of information technology enables anyone—from an individual to a nation state—to target a victim halfway around the world at minimal cost and with little risk of being caught. Because the cost of failure is minimal, the threat evolves rapidly. In contrast, the costs of defense, as well as potential consequences, are significant.

Because this asymmetric threat is rooted in the fundamental structure of the Internet and information technology, there is no way to solve cybersecurity without undermining the benefits of the cyberspace. There is no silver bullet or technological solution. While we certainly can do more improve the security of cyberspace, these decisions require a thoughtful cost benefit analysis. How will a potential security measure affect the cost or convenience of a product? How will it affect the pace of innovation? What will it mean for privacy or civil liberties?

Cyberspace is no longer a place that we visit. It is a place where we live. Ten years ago, smartphones were a novelty—in fact, the iPhone didn't even exist. Today, mobile devices serve as a credit card, track our health, unlock our homes and start our vehicles. A pacifier can monitor your infant's temperature and send that information directly to your computer or mobile device. Through connected kitchen appliances, you can start dinner from the office, check social media accounts from your grill or know when you're low on milk. Cyberspace is, and will increasingly be, the economic engine of the 21st century economy.

At the same time, as the Internet and information technology become increasingly entwined in our daily routines, cyberspace becomes a limitless and adaptive attack surface. The security challenges will be more diverse and harder predict. And the consequences will be more severe. We may not be able to secure cyberspace but it is our collective responsibility to understand the threat in order to minimize its effect on our privacy, civil liberties, national security and economic prosperity.

I encourage all my colleagues, on both sides of the aisle, to embrace the unique opportunity this hearing presents. We are not here to debate data breach legislation or other specific policy issues. We are privileged to have an impressive panel of experts who can help us understand the challenge of cybersecurity in context. I look forward to hearing from each of our witnesses and the unique perspectives they bring to this important discussion. In particular, I want to recognize Dr. Shannon from Carnegie Mellon University, which is home to the nation's first computer emergency response team. The Pittsburgh region boasts some of the nation's foremost experts in the field of cybersecurity, and I am pleased to have one of those experts, Dr. Shannon, joining us here today.

Mr. MURPHY. I will now recognize the ranking member of the O&I Subcommittee, Ms. DeGette of Colorado, for 5 minutes.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Thank you, Mr. Chairman. I am glad we are having the time to do a deep dive into this important topic. O&I has a long history of exploring issues related to cybersecurity. Over the years, we have had hearings on cybersecurity risks. We have passed bipartisan legislation to promote security and resiliency for critical infrastructure systems. We have also examined in detail both cyber attacks and vulnerabilities within many of the sectors under this committee's jurisdiction. I hope that this series of hearings will help us have additional productive conversations about how both to understand the cyber risks and how to respond to them.

Information systems connected to the Internet are integral to the operation of our economy. While this interconnectedness is essential, the vulnerabilities that it can pose, pose serious challenges. Every day, the Internet is under attack by those with malicious intent. In the last few years, cyber attacks on federal agencies and also on private entities have skyrocketed. Every week it seems, there is a new series of headlines about cyber attacks and vulnerabilities in our system. Last week, for example, Uber revealed a breach of its driver database that had gone unreported for months. Anthem reported that millions of people who were not its customers could be victims of cyber attacks on their systems. Last year, we heard of attacks on Home Depot, Target, and JP Morgan Chase that involved the personal information of tens of millions of Americans.

So this past year alone has been a stark reminder that all industries are vulnerable, and neither the private sector or government is safe from cyber attacks. These attacks are becoming more and more frequent, and more and more sophisticated. I am personally concerned about how the loss of personally identifiable information is affecting American consumers. It is starting to appear that there are two types of these Americans. Number one, people whose data has been subject to a breach, and number two, people whose data will be subject to a breach. That seems to be how it is breaking out.

So I look forward to hearing from our witnesses today about the cybersecurity landscape. I have a couple of questions. Number one, what are the threats that we now face, and number two, what are our biggest vulnerabilities. Also, I want to hear what we are doing now, and what we can improve in the future. What are the existing standards in both the government and private industry for keeping personal information safe, and providing notification when there is a breach. How can we make sure that both the public and private sectors are using their expertise to ensure that cybersecurity measures are appropriately tailored to address the specific needs in the different sectors. More fundamentally, what is the appropriate role of government and of the private sector in securing the systems, managing cyber risks, and assessing cyber threats. How do we promote the optimal level of cooperation and information sharing within this division of labor. Unfortunately, this is a problem that doesn't have an immediate or a fissile solution.

So I am hoping that our witnesses throughout the hearings can advise us on how we can make the right strategic investments in cybersecurity in both the short and long-term. They are all smiling because they know what an impossible task this is. But this is a problem that exists far beyond our Nation's borders. We should be thinking about how we can ensure international cooperation to protect against cyber threats around the world. I understand we need to make substantial changes in the way we think about cybersecurity. This is not a problem that we have the tools to deal with immediately. And I do want to hear from our witnesses about that today, but even while we rethink our approach to cybersecurity and make necessary long-term investments, I want to know what we can do right now to protect consumers and their personal information. If data breaches have become inevitable, we need to think about how to make that data unusable once it is stolen, and that seems to be a short-term key. I want to hear from the witnesses about creative solutions in the post-breach environment. On the battlefield, a strategy for preventing the enemy from successfully using your technology against you is to render it useless if it falls into the wrong hands. I think we need to figure out ways to do this now with certain types of consumer information if it is stolen.

As Chairman Murphy said, this is just the first in a series to explore cyber threats in a variety of sectors. I want to thank the witnesses, and I look forward to our continued work.

I yield back.

Mr. MURPHY. Gentlelady yields back.

Now recognize the vice chair of the full committee, Mrs. Blackburn of Tennessee, for 5 minutes.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. Thank you, Mr. Chairman, and thank you for the attention to this issue. And witnesses, we appreciate that you are here as we begin to think through this process.

Cyberspace is really a place where a lot of our information now resides. It is not just something that we click onto and off of, but it is a place of residence for what I term our virtual you, which is you and all of your information. And interestingly enough, and the chairman noted the end-to-end open architecture of the system, the backbone that permits this, and you do have that original platform, that openness, which makes it what it is, and makes it a successful information service. So now, we have all of these incursions, and the malware and the spyware and the bots, and this and that, and some of these are embedded in hardware, some are there via software, and we are looking at an increased number of these attacks on our critical infrastructure every day.

Now, the chairman mentioned a little bit about the Internet of things, or as I like to say, the Internet of everything. And we know that by the end of this decade, Sysco says we are going to have 50 billion, 50 billion devices that are connected to the Internet. That is a lot of vulnerabilities. So as we look at the steps that need to be taken for privacy and for data security, we welcome your expertise and your insights, and we thank you for helping us think forward on this.

And I yield at this time to Dr. Burgess.

Mr. BURGESS. I thank the vice chairwoman for yielding. Chairman Murphy, thank you for having the subcommittee have this hearing on reviewing the current state of cybersecurity. It is an issue that is vital to the future of commerce and our economy. Developing a strong grasp of the engineering and technical realities underpinning computer networks, and what that means for business models is an integral part of understanding cybersecurity.

I do want to acknowledge, Chairman Murphy, your comments that this is not a data breach hearing. The Subcommittee on Commerce, Manufacturing and Trade is working to finalize legislation establishing a data security requirement, and a single set of breach notification rules for entities under the Federal Trade Committee's jurisdiction. But that is just one piece of the broader puzzle, and I look forward to the broader discussion of cybersecurity at today's hearing.

Thank you, Mr. Chairman. I will yield back the balance of the time.

Mr. MURPHY. Thank the gentleman.

And now I turn to Mr. Pallone for 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman.

I want to borrow the words of one of our witnesses here today. Dr. Shannon, in summarizing the cybersecurity landscape, says this in his written testimony, and I quote, “Currently there is no manner in which an entity, public or private, can be fully protected without simultaneously destroying its value. Today, there are neither the tools, technology, nor resources to stop all serious cyber attacks and allow for efficient function of electronic commerce. We simply do not yet know how to do both of these together, which makes enabling continued technology research an innovation essential.” and that is the end of his quote.

Dr. Shannon, you captured perfectly the problems we face in this area, and the challenges in responding. This committee has a long history on cybersecurity issues, and I look forward to this series of hearings as we continue to examine this area.

Unfortunately, our ability to protect against cyber attacks while improving still appears to lack what is needed to prevent these intrusions. We are seeing more frequent and more severe attacks in both the public and private sectors. In just the past few years, millions of Americans have had their information compromised in data breaches. At the same time, our dependence on the Internet and interconnected information systems has only increased. Disconnecting from the Internet is not an option for a vast majority of individuals and companies alike.

The private sector seems to be no better at preventing attacks than the Federal Government. In the last year or so, we have seen breach after breach where attacks are placing Americans’ personal data at risk. Attacks on Target, JP Morgan, Home Depot, Sony, and now Anthem have all underscored this fact. And these attacks illustrate that even the biggest companies with considerable resources at their disposal are not immune to these intrusions. We must also face the reality that it is much cheaper for the attackers to infiltrate than it is for us to protect and respond, and unfortunately, there is no one solution at this time to guarantee that stored information will remain secure. But we can’t ignore cybersecurity until we have a solution. Instead, we need to find ways to manage the problem, and I hope this series of hearings can bring out some creative solutions on how to do just that.

In addition, we need to start thinking about post-breach protections, particularly as it relates to consumers. Clearly finding ways to strengthen existing systems is necessary, but we also need to make it harder for thieves to use stolen data after breaches occur. It is not enough for companies to simply offer a free year of credit monitoring as an answer. Rather, we need to explore ways to make consumer data less useful if it falls into the hands of the bad guys.

So, Mr. Chairman, coming up with effective solutions to these problems will be a long process, but I applaud you and our ranking member, Ms. DeGette, for starting this series of hearings, and I look forward to working with you to better protect our institutions, companies, and citizens.

I yield the remaining of my time to the gentlewoman from New York, Ms. Clarke.

Ms. CLARKE. I would first like to thank both our Chairman Murphy and Ranking Member DeGette for having this hearing, and I would like to thank the gentleman from New Jersey, the ranking member of our full committee, Mr. Pallone, for yielding me time.

I thank our witnesses for lending their expertise, time, and talent to today's Oversight and Investigations hearing.

As you know, I was on the Homeland Security Committee for the past 8 years, and of those 8 years, I was ranking member of the Cybersecurity and Critical Infrastructure Subcommittee for 4 years, and chairwoman for 2 years. Needless to say, this issue is extremely important to me, but more importantly, to our Nation. There is no doubt that we face a challenge of incredible proportions when it comes to cyber threats. Comprehensive and effective cybersecurity policy has always been a complicated endeavor, but in the face of the technological landscape that is constantly evolving and developing new mechanisms that threaten the integrity of our Nation's virtual presence, we stand in unchartered territory as we try to shape a government and corporate response that is effective, adaptable, and a step ahead of any threat we may encounter.

We hear about a new breach in security or impending cyber threat almost daily, so it is inarguable that the time to set our House in order has come and it is now. The security of our Nation's cyber infrastructure and our response to cyber threats is not a partisan issue. We have to work together: democrats and republicans, government and private industry, academics and public advocates, to not only protect the privacy of our citizens, but also identify and respond to security threats. Ultimately, however, it is the expertise of today's witnesses, and many others across the cyber community, that will allow us to act in the best interests of our Nation.

I look forward to listening to and learning from what today's witnesses have to share with us.

I yield back to Ranking Member DeGette.

Mr. DEGETTE. I yield back.

Mr. MURPHY. All right, thank you. Thank you.

We are expecting votes from between 2:15 and 2:45, so we will move quickly through these questions. 2:45, 3:15? All right, 2:45, 3:15, so we should have plenty of time.

So now let me introduce the witnesses on the panel for today's hearing. First, Dr. Herbert Lin, Senior Research Scholar for Cyber Policy and Security at the Center for International Security and Cooperation, a Senior Fellow at the Hoover Institute in Stanford University, his research relates broadly to policy-related dimensions of cybersecurity and cyberspace, and particularly interested and is knowledgeable about the use of offensive operations, cyberspace, especially instruments of national policy. Welcome here, Dr. Lin.

Next, Dr. Richard Bejtlich. I say that right?

Mr. BEJTLICH. Yes, sir.

Mr. MURPHY. Good. Is the chief security strategist at FireEye, Incorporated, and was Mandiant's chief security officer when FireEye was acquired by Mandiant in 2013. In this role, he empowers policymakers, international leaders, global customers, and concerned citizens to understand and mitigate digital risks through strategic security programs.

Our third panelist is Dr. Greg Shannon, Chief Scientist for the CERT Program at the Software Engineering Institute at the Carnegie Mellon University. In this role, he is responsible for working with the director and SEI leadership to plan, develop, and implement research strategies, initiatives, and programs that further the mission of CERT and SEI, as well as developing, conveying, and executing innovative ideas for the Nation's cybersecurity research agendas. In addition, he was recently named chair of the Institute of Electrical and Electronics Engineers Cybersecurity Initiative.

I will now swear in the witnesses. As you all are aware, the committee is holding an investigative hearing, and when doing so, has the practice of taking testimony under oath. Do any of you have objections to testifying under oath? Seeing no objections, the chair then advises you that under the rules of the House and the rules of the committee, you are entitled to be advised by counsel. Do any of you desire to be advised by counsel during your testimony today? And they have all indicated no. In that case, would you please rise and raise your right hand, I will swear you in.

[Witnesses sworn.]

Mr. MURPHY. Thank you. All the witnesses answered in the affirmative. So you are now under oath and subject to the penalties set forth in Title XVIII, section 1001 of the United States Code. We will recognize you each for a 5-minute summary. The rules are press the button on the mic, pull it close to you. Watch for the red light, that means your time is up.

Dr. Lin, you may begin.

TESTIMONY OF HERBERT LIN, SENIOR RESEARCH SCHOLAR, CENTER FOR THE INTERNATIONAL SECURITY AND COOPERATION, SENIOR FELLOW, HOOVER INSTITUTION, HARVARD UNIVERSITY; RICHARD BEJTLICH, CHIEF SECURITY STRATEGIST, FIREEYE, INCORPORATED; AND GREGORY SHANNON, CHIEF SCIENTIST, CERT PROGRAM, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY

TESTIMONY OF HERBERT LIN

Mr. LIN. Mr. Chairman, members of the subcommittee, thanks for the opportunity to testify. Testimony today is personal, although my professional work informs it.

Let me start with two definitions. Cyberspace is computers, smartphones, the Internet, stuff with computers inside them. It is also the information inside these things, and our dependence on all of this is growing.

Here is a definition of cybersecurity that—with words like negative impact and bad guy. What is important here is that the definitions of these words are policy matters, and also cybersecurity isn't just technology. Economics, psychology, organizations, they all matter because they help to shape user behavior, which affects cybersecurity.

On security, a computer in a sealed metal box, there is supposed to be a computer inside that one on the left. There is one on mine. And it is a sealed metal box, so I guess you can't see it. That is perfectly secure, but it is useless. OK. The one on the right is useful but potentially insecure because—it is useful because you get information in and out of it. You only want good data to get into it. That requires a judgment about what counts as good, and such judgments are fallible.

Here is a network of nodes that represents the Internet. At each node there is another network or a computer. The Internet is designed with just one function really; to transport data from A to B without regard for what it means. Usefulness of the Internet comes from the computers that sit at the nodes, and this principle is what has really enabled the Internet to grow so quickly in the past. But if you believe in this principle, it also means that the network in the middle doesn't handle security. Many people want to put security in the middle, but that would violate this basic principle that has driven Internet growth and innovation, and also the change wouldn't entirely solve the cybersecurity problem. There are some exceptions to this description, but they don't really change the basic story.

Complexity is the enemy of cybersecurity. What we want from our computers requires complex systems. We put components into a system. When the system is complex enough, nobody understands the system very well, and so the system, in fact, may not be secure. And here is an example of complexity at work. You have done this before, from a browser you type in the URL, like EnergyCommerce.House.gov, and then in less than a second the E&C Commerce site appears. OK. This is what is going on behind the scene. It is not worth going over each of these elements, I don't have time for it either, but at every one of these boxes, an adversary could interfere with your Web experience.

Also, adversaries adapt, and here is an example from safecracking. Good guys don't get the last move here. When we put money in wooden boxes to protect them, robbers use axes. When we used metal safes to stop them, they drilled wedges between the door and the safe. When you put in step doors, they poured in nitroglycerine, and so on. And we still haven't entirely stopped bank robberies.

The result of this is this chart. Over time, we get better at cybersecurity, that is the bottom line, but the top line, how much we depend on cyberspace and, therefore, how much the threat that we face has grown even faster, and that gap, therefore, is growing. The defenses of today would be good against the threats of 10 years ago, but the threat has changed too.

This leads to conclusion one, which is that cybersecurity is a never-ending battle. You will not find a decisive solution forever, and so you have to find ways to manage it at an acceptable cost. This really leads to two questions: why bother with cybersecurity at all, and how can we manage the problem? On the why bother, here are some reasons. You deal with the unsophisticated threats, you make yourself less vulnerable so the bad guys go after the next guy rather than you. You can give the bad guy less time to do his dirty work, and you help law enforcement focus on the harder cases. OK. Second, why is it so hard to solve this as a policy problem? Well, the reason is that we want cybersecurity, but we want other good things as well. We want rapid innovation, and it is always faster to do something without attention to security. We want convenience on cybersecurity. It mostly gets in your way. How often have you been at a computer that you couldn't get on because you forgot a password? There is also interoperability, which means sometimes you can't fix a known security problem because you are afraid of damaging existing programs. And we want privacy for us but not the bad guys. That means when we try to collect data on the bad guys, sometimes we collect data inadvertently on the good guys. And the tradeoff is that we don't know how much inadvertent collection we should tolerate to gain security. Tradeoffs are unavoidable, and that means it makes consensus hard to reach. How do you do better? Well, part one is you reduce the gap between the average and the best, and part two is you reduce the gap between the best and what you actually need.

So here is my summary of this, which is all in your—this is a one-page summary. And this reference, from which much of this testimony is drawn, I would like to incorporate that into the record of the hearing, if I may. And I think it has been distributed to members. So that is it. Thank you.

[The prepared statement of Mr. Lin follows:]

Testimony by Herbert Lin

Senior Research Scholar, Center for International Security and Cooperation

Research Fellow, Hoover Institution

Stanford University

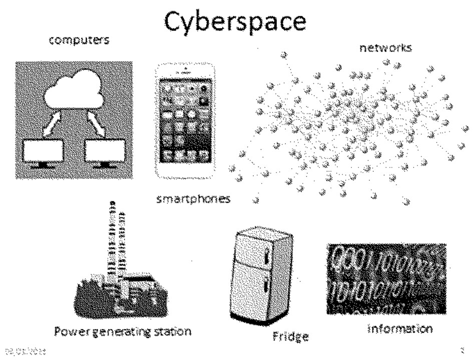
Chief Scientist (Emeritus), CSTB, National Research Council

House Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

March 3, 2015

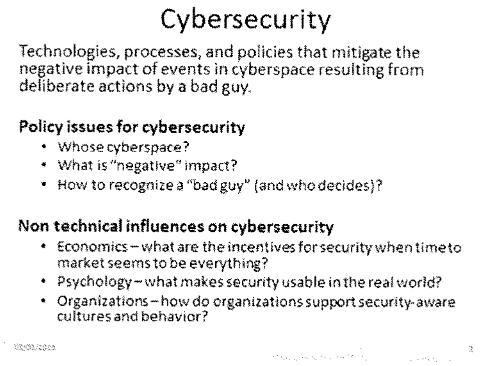
Fundamental cybersecurity challenges to public policy



Cyberspace

Cyberspace includes computers, networks including but not limited to the Internet, things connected to the Internet, and things with computers embedded inside them as well as the information that these technological artifacts use, store, handle, process, or transmit. And our society is becoming more and more dependent on cyberspace.

14



Cybersecurity

Technologies, processes, and policies that mitigate the negative impact of events in cyberspace resulting from deliberate actions by a bad guy.

Policy issues for cybersecurity

- Whose cyberspace?
- What is "negative" impact?
- How to recognize a "bad guy" (and who decides)?

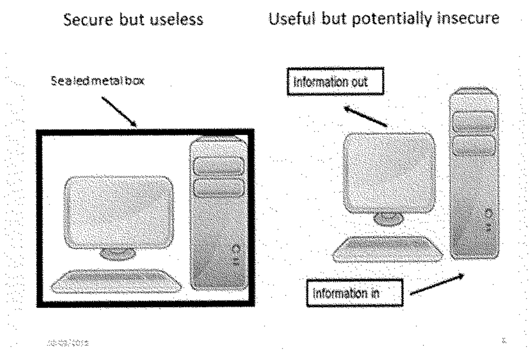
Non technical influences on cybersecurity

- Economics – what are the incentives for security when time to market seems to be everything?
- Psychology – what makes security usable in the real world?
- Organizations – how do organizations support security-aware cultures and behavior?

Cybersecurity consists of technologies, processes, and policies that mitigate the negative impact of events in cyberspace resulting from deliberate actions by a bad guy. Note that this definition begs important questions, such as "whose cyberspace" (a company's? a nation's? an agency's?), what counts as "negative impact", and how we recognize a "bad guy"? All of these questions, of course, are policy questions rather than technical ones.

Also, cybersecurity is not just technology. Economic issues play out when vendors of products and services have to move very quickly in a very competitive market when time-to-market is everything in building a business and the imperative for speed precludes spending time on security. Psychology is apparent when you look at what makes security usable in the real world. For example, many passwords are easily guessed, and yet passwords have stuck around for decades even though we know how to do better. Why don't we? In large part, it's because these better methods are more of a hassle or cost more to use. Organizations and their cultures can shape behavior as well. For example, an organization that penalizes users for bad security behavior and one that rewards good security behavior are different, and the security posture of each organization may well be different.

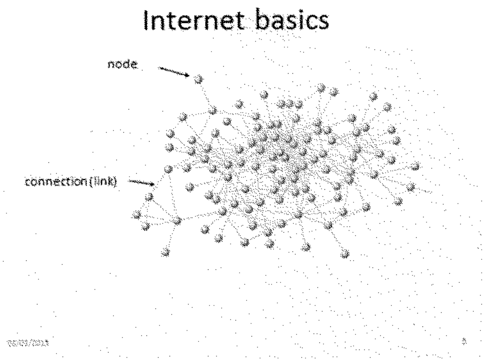
15



Secure but useless

Useful but potentially insecure

Perfect security is possible only if you make the computer useless. We see a computer in a sealed metal box – you can't hack it, but you also can't use it for anything. Once you allow information (to include both data and programs) in, someone must make a judgment about what information counts as "good"—and that judgment is fallible, especially against a smart adversary. Computers generally can't do it as well as people can, and people do make mistakes in judgment as well.



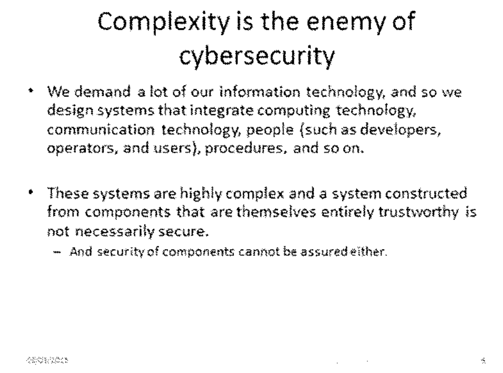
Internet basics

The Internet can be regarded as a network of nodes. At each node is a computer or another network. Roughly, the Internet has been designed to have just one function—to make its best effort to transport information from A to B—and the technology does not care about the nature of that information. Furthermore, it is deliberately designed to put all of the useful functionality that you and I expect from computers at the end nodes. The internet was originally designed to be an unregulated marketplace in which anyone with a good idea could put up an application at some node with minimal regulatory burden—and this design principle is what enabled to the Internet to grow so fast in the past 30 years.

With this design, security issues must be handled at the end nodes rather than in the middle. One could, in principle, change the Internet's architecture to require that security issues per se to be handled internally, but this change would drastically reshape the nature of the Internet experience for those developing end-user applications, subjecting them to a far higher degree of interference with the traffic they want to send and receive, and likely reducing the freedom they have to innovate. Also, this change alone would not be likely to solve the entire cybersecurity problem, as it would not improve the security of the systems connected to the end nodes.

There are modest exceptions to the description provided above, but they do not change the basic story line.

17



Complexity is the enemy of cybersecurity

- We demand a lot of our information technology, and so we design systems that integrate computing technology, communication technology, people (such as developers, operators, and users), procedures, and so on.
- These systems are highly complex and a system constructed from components that are themselves entirely trustworthy is not necessarily secure.
  - And security of components cannot be assured either.

Complexity is the enemy of cybersecurity. We ask a lot of our information technology, and to get that functionality, we have to integrate many different components. We put these components into a system, and when the system is complex enough, no one understands that system very well. And so even if the components are themselves individually secure (and they are not), the system may not in fact be secure.

There's a sense in which it's a lot like crafting good legislation and regulation. For example, you know how hard it is to develop legislative language that covers every possible case. Often, new legislative language may interact with other legislative language already on the books, resulting in some surprising and undesirable outcomes. Then you need to pass even newer legislation to fix those problems—in the computer world, that's called a bug patch.

The next several slides provide an example of how complexity manifests itself.

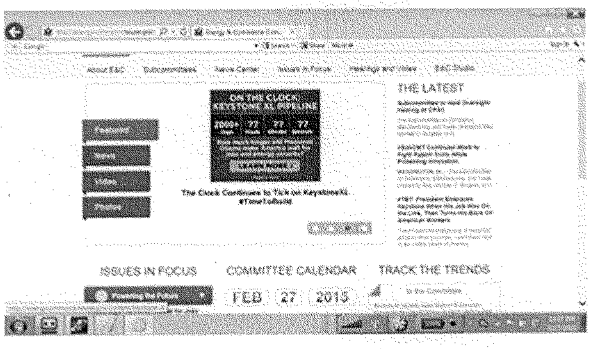
18

Viewing a Web Page (from the user's perspective)

03/03/2015

Here, we type in the name of a web page, and the page usually appears in the next slide in less than a second.

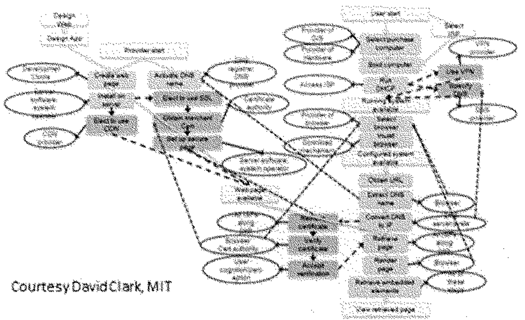
View Page Here



And here it is.

20

Viewing a Web Page (behind the scenes)

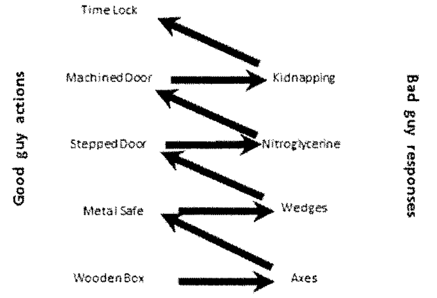


Courtesy David Clark, MIT

This is what is going on behind the scenes. It's not worth going over every one of these elements, but it's obvious that behind the scenes is a great deal of complexity. Every one of these rectangular boxes is a place where a bad guy can take a deliberate action to interfere with your web experience.

21

Adversaries adapt: an example from safecracking



Good guy actions

Time Lock

Machined Door → Kidnapping

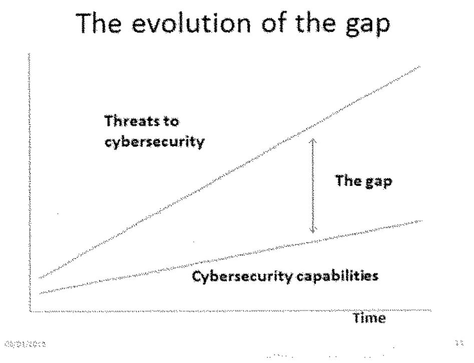
Stepped Door → Nitroglycerine

Metal Safe → Wedges

Wooden Box → Axes

Bad guy responses

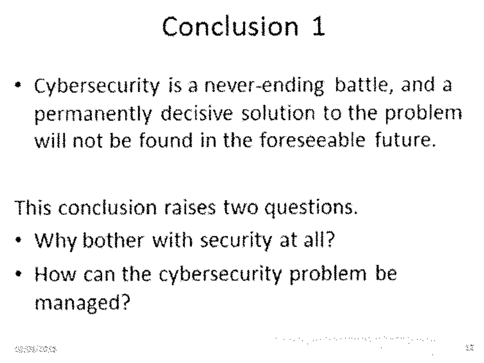
Also, adversaries adapt. They are smart, and the good guys don't get the last move. Indeed, there is no last move. Reading the slide from the bottom up, the good guy does what's on the left and the bad guy responds by doing what's on the right. And note that, in the physical world, we still haven't entirely stopped bank robberies – and now the bad guys have moved to the Internet to rob banks.



The evolution of the gap

Here's the net result. It's true that over time we have gotten better at cybersecurity—that's the bottom line. But the top line – how much we depend on cyberspace – has grown even faster, and with that growing dependence the threats have grown commensurately.

23



Conclusion 1

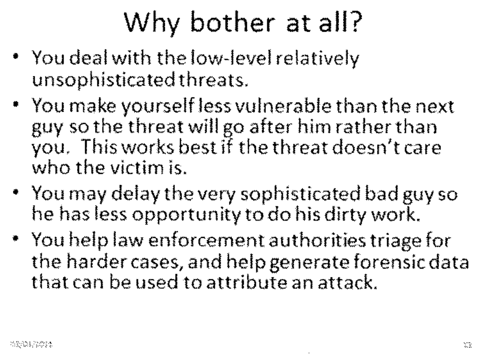
- Cybersecurity is a never-ending battle, and a permanently decisive solution to the problem will not be found in the foreseeable future.

This conclusion raises two questions.

- Why bother with security at all?
- How can the cybersecurity problem be managed?

Based on previous slides here's the first basic conclusion – Cybersecurity is a never-ending battle, and a permanently decisive solution to the problem will not be found in the foreseeable future. Thus, the public policy question is not how the cybersecurity problem can be solved, but rather how it can be managed at an acceptable cost in dollars and effort expended by the various stakeholder parties who have something to lose.

This conclusion leads to two important questions.

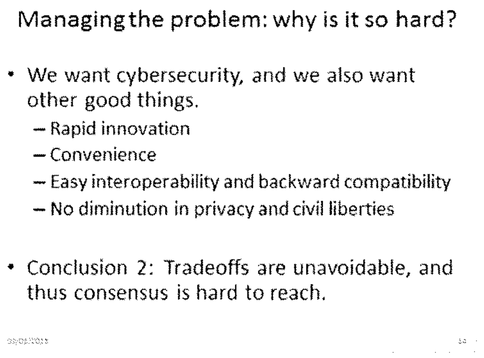


Why bother at all?

- You deal with the low-level relatively unsophisticated threats.
- You make yourself less vulnerable than the next guy so the threat will go after him rather than you. This works best if the threat doesn't care who the victim is.
- You may delay the very sophisticated bad guy so he has less opportunity to do his dirty work.
- You help law enforcement authorities triage for the harder cases, and help generate forensic data that can be used to attribute an attack.

Given this conclusion, Slide 13 asks and answers the first question – why bother? If the good guys will never win decisively, what is the point? There are at least 4 reasons:

- You deal with the low-level relatively unsophisticated threats.
- You make yourself less vulnerable than the next guy so the threat will go after him rather than you. This works best if the threat doesn't care who the victim is. If he cares a lot, this won't work at all because he will try again and again. (A consequence of this point is that if the US government has information that can be obtained only from the government, the bad guys won't go elsewhere.)
- You delay the sophisticated bad guy so he has less opportunity to do his dirty work and make it more expensive for him, so he can do less of it.
- You help law enforcement authorities do triage for the harder cases, and you generate data that can help with forensics supporting attribution of an attack.



Managing the problem: why is it so hard?

- We want cybersecurity, and we also want other good things.
  - Rapid innovation
  - Convenience
  - Easy interoperability and backward compatibility
  - No diminution in privacy and civil liberties

- Conclusion 2: Tradeoffs are unavoidable, and thus consensus is hard to reach.

03/03/2015 14

Question 2 is how we should manage cybersecurity as a public policy problem, and why is it so hard?

The fundamental reason is that we want cybersecurity, yes, but we also want many other things.

We want rapid innovation, and it's always easier and faster to do something without paying attention to security. And in a world in which being first to market has many economic advantages, it's entirely rational from a developer's point of view to ignore security at the start when the concept has yet to be proven. And once the concept has been proven, the right thing to do from a security standpoint is to start over again, this time integrating security into it.

But few people work like that. What they do, if they do anything, is to treat security as an add-on—and any design decisions they made with bad security consequences don't get fixed.

From a user standpoint, this is also rational behavior, at least in the short-term. They get a new application that does something useful for them. They don't face much of a threat because the application is new, and few hostile parties know about it, so the security environment is relatively benign.

As the app grows in popularity, so do the incentives for hacking—and so the threat grows. But now the developer is *really* locked into his original design, because changing it now runs the risk of starting over again and losing his (large) customer base. So he is forced into a situation of patching – fixing problems as they appear.

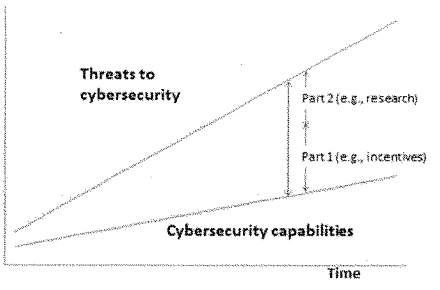
Users also value convenience, and cybersecurity measures are the antithesis of convenience—mostly, cybersecurity gets in the way of doing useful work. How often have you been kept off your computer because you forgot a password? The whole point of security is to make your computer totally inaccessible to a bad guy trying to pretend he is you, and sometimes the automated mechanisms set up to differentiate you from a bad guy don't work so well.

The same is true about interoperability and backward compatibility. As you use an application, you become familiar with it. When you upgrade, you don't want to lose your investment in it, e.g., you don't want to be unable to use your old data files with the upgrade. But sometimes it happens that putting in backward compatibility means that you can't fix a known problem in the upgrade, because if you fix it, you'll break something else that depended on that problem being present.

And we cherish our privacy and civil liberties as law-abiding Americans—but not for the bad guys. Again, sometimes it's hard to tell the difference, especially since smart bad guys try to look like law-abiding Americans. As we try to collect data that will help to identify bad guys in cyberspace, we sometimes gather data—inadvertently—on good guys. That is, we unintentionally violate their privacy rights and their civil liberties. This tradeoff is also unavoidable—we have to decide how much inadvertent violation we are willing to tolerate in order to gain whatever security benefits we are seeking, and we have no consensus on how far we're willing to go.

All of these examples lead to Conclusion 2: Tradeoffs are unavoidable, and thus the consensus needed to take action is hard to reach.

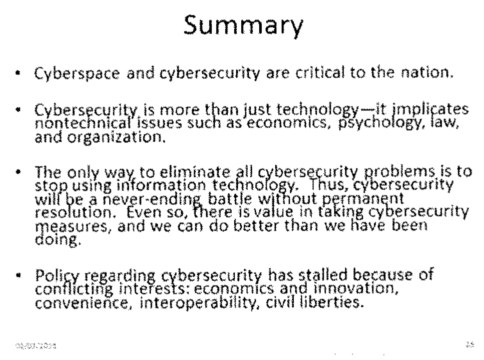
Doing better



Reducing the gap is a two-part effort. Part 1 says we should reduce the gap between the average cybersecurity posture and the best possible cybersecurity posture. Part 1 is primarily nontechnical in nature, involving things like developing incentives to use known and better technologies and practices and applying already-known technical knowledge about cybersecurity.

Part 2, which we do simultaneously with Part 1 says we should reduce the gap between the strongest posture possible with known practices and technologies and the actual need. Part 2 is primarily technical, and involves developing new knowledge about cybersecurity.

28

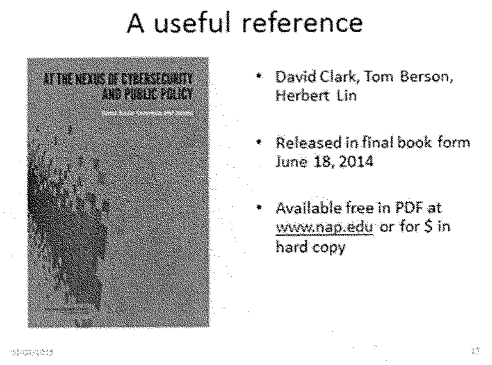


Summary

- Cyberspace and cybersecurity are critical to the nation.
- Cybersecurity is more than just technology—it implicates nontechnical issues such as economics, psychology, law, and organization.
- The only way to eliminate all cybersecurity problems is to stop using information technology. Thus, cybersecurity will be a never-ending battle without permanent resolution. Even so, there is value in taking cybersecurity measures, and we can do better than we have been doing.
- Policy regarding cybersecurity has stalled because of conflicting interests: economics and innovation, convenience, interoperability, civil liberties.

03/03/2015 28

This is the one page summary of my key points.



A useful reference

- David Clark, Tom Berson, Herbert Lin
- Released in final book form June 18, 2014
- Available free in PDF at www.nap.edu or for $ in hard copy

03/03/2015 17

A reference to be incorporated to the hearing record.

[The attachment to Mr. Lin's testimony has been retained in committee files and can be found at *http://docs.house.gov/meetings/if/if02/20150303/103079/hhrg-114-if02–20150303-sd006.pdf.*]

Mr. MURPHY. Thank you.

Now our next witness, go ahead, 5 minutes.

TESTIMONY OF RICHARD BEJTLICH

Mr. BEJTLICH. Chairman Murphy, Ranking Member DeGette, members of the committee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. Today I will discuss briefly digital threats, how to think about risk, and some strategies to address these challenges.

So first, who is the threat? We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, Syria, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain. The Iranians and North Koreans extend these activities to include disruption via denied service and sabotage using destructive malware. Activity from Syria relates to the regional civil war, and sometimes affects Western news outlets and other victims. Eastern Europe continues to be a source of criminal operations, and we worry about the conflict between Ukraine and Russia extending into the digital realm.

I began by saying who is the threat, and that brings about threat attribution. Threat attribution, or identifying responsibility for a breach, depends on the political stakes surrounding an incident. For high-profile intrusions such as those in the news over the last few months, attribution has been a priority. National technical means, law enforcement, and counterintelligence can pierce anonymity. Some elements of the private sector have the right experience and evidence to assist with this process. So attribution is possible, but it is a function of what is at stake.

So who is being breached? In March of 2014, the Washington Post reported that in 2013, federal agents, most often the FBI, notified more than 3,000 U.S. companies that their computer systems had been hacked. This count represents clearly identified breach victims. Many were likely compromised more than once. How do victims learn of a breach? In 70 percent of the cases, someone else, likely the FBI, tells a victim about a serious compromise. Only 30 percent of the time, the victims learn of the intrusions on their own. The median amount of time for when an intruder first compromises a victim to when the victim learns of a breach is currently 205 days. This means that, unfortunately for nearly 7 months after gaining initial entry, intruders are free to roam within victim networks.

Well, what is the answer? Before talking about solutions to digital risk, we need to define it. Always ask risk of what. Are we talking about the risk of a teenager committing suicide due to cyberbullying, or the risk of a retiree's 401(k) being emptied due to electronic theft, or the risk of a week-long power outage due to state-sponsored attack? Step one is to define the risk, and step two is to measure progress by combining means and ways to achieve defined ends.

To measure success, I recommend that a security team track the number of intrusions that occur every year, and you will see this in the FISMA report that was just released yesterday, although, honestly, it seemed buried in the report. So you want to count the number of intrusions per year, but more importantly, you want to measure the amount of time from when the intruder first gets into the enterprise to when someone notices, and when from someone notices to when you kick them out. And these are the metrics that I don't see recorded too often.

It is also important to think in terms of how to define risk, and security professionals, like the ones at this table, tend to think in terms of threat vulnerability and cost. And we use a pseudo equation where risk is the product of threat vulnerability and cost. We are not trying to calculate a number; just show that, as you influence each one of these factors, you either raise risk or lower risk.

So I think in general, there is a lot of attention paid to the vulnerability in a computer and an iPhone, that sort of thing, but we need to spend a lot of time as well on the threat and the cost. Law enforcement and counterintelligence are the primary means by which you can mitigate the threat. In an editorial for Brookings that I wrote, I asked what makes more sense; expecting two billion Internet users to adequately secure their personal information, or reducing the threat posed by the roughly 100 top tier malware authors? So that is the threat side.

On the cost side, we need to think of ways to reduce the cost of dealing with a security breach, not only for companies but also for consumers. So we are seeing this in a couple of different areas. One step in place is the tokenization of payment card system data where you replace a credit card number with a string of numbers in its place. A second step would be eliminating the value of the social security number to identity thieves. I recommend reading the Electronic Privacy Information Center suggestions on effective social security legislation for some policy changes.

In brief, defenders win when they stop intruders from achieving their objective. It is ideal to stop the adversary from entering the network, but that goal is increasingly difficult. I recommend you quickly detect the intrusion, respond to contain the adversary, and then kick them out.

And finally, we must appreciate that the time to find and remove intruders is now. There is no point in planning for future theoretical breaches. If you were to hire me to be your chief security officer, the very first step I would take would be to hunt for intruders already in the network.

I look forward to your questions.

[The prepared statement of Mr. Bejtlich follows:]

Statement for the Record

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

Before the

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

Understanding the Cyber Threat

and Implications for the 21st Century Economy

March 3, 2015

Chairman Murphy, members of the Committee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution, and I am pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center.

My employer, FireEye, provides software to stop digital intruders, with 3,100 customers in 67 countries, including 200 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions.

Today I will discuss digital threats, how to think about risk, and some strategies to address these challenges.

Who is the threat?

We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, Syria, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain. The Iranians and North Koreans extend these activities to include disruption via denial of service and sabotage using destructive malware. Activity from Syria relates to the regional civil war and sometimes affects Western news outlets and other victims. Eastern Europe continues to be a source of criminal operations, and we worry that the conflict between Ukraine and Russia will extend into the digital realm.

Threat attribution, or identifying responsibility for a breach, depends on the political stakes surrounding an incident.[1] For high-profile intrusions, such as those in the news over the last few months, attribution has been a priority. National technical means, law enforcement, and counter-intelligence can pierce anonymity. Some elements of the private sector have the right experience and evidence to assist with this process. Attribution is possible, but it is a function of what is at stake.

Who is being breached?

[1] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," The Journal of Strategic Studies, 2014; http://bit.ly/attributing-cyber-attacks

In March 2014, the Washington Post reported that in 2013, federal agents, often the FBI, notified more than 3,000 U.S. companies that their computer systems had been hacked.[2] This count represents clearly identified breach victims. Many were likely compromised more than once.

Serious intruders target more than government, defense, and financial victims. No sector is immune. FireEye recently published two reports, showing that 96% of organizations we could observe had suffered compromise during two six-month periods.[3] The best performing sector was aerospace and defense, with "only" 76% of sampled organizations suffering a breach. All of the retail, automotive, transportation, healthcare, pharmaceutical, construction, and engineering clients we passively monitored over a six-month period were breached at least once.

In 2014, the top sectors assisted by our Mandiant consultants included business and professional services, finance, media and entertainment, and construction and engineering. Many of these attacks are driven by strategic national imperatives. For instance, we anticipate that certain foreign governments will continue to steal clean energy and biotechnology solutions, so long as their citizens suffer polluted cities and rising cancer rates. Some actors specifically target the healthcare sector. Criminal groups appear to steal data for financial gain, while nation-state hackers may steal data to improve the healthcare systems of their own countries, or to support national commercial champions.

How are victims breached?

Intruders use spear phishing, attacks against Internet-connected devices, and other methods to compromise victims. Last year we observed a rise in the proportion of phishing emails that impersonated IT staff, from 44% in 2013 to 78% in 2014.[4] The threat is going mobile as well. We recently completed a study of vulnerable mobile applications that can hijack entire devices, without the user's knowledge. We have seen malicious applications, pretending to offer banking services, harvest credentials and steal two-factor authentication codes and virtual private network passwords.

[2] Ellen Nakashima, "U.S. notified 3,000 companies in 2013 about cyberattacks," Washington Post, March 24, 2014; http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html

[3] https://www.fireeye.com/blog/executive-perspective/2015/01/the_maginot_linedee.html

[4] https://www.fireeye.com/blog/threat-research/2015/02/get_a_view_from_the.html

How do victims learn of a breach?

In 70% of cases, someone else, likely the FBI, tells a victim about a serious compromise. Only 30% of the time do victims identify intrusions on their own. The median amount of time from an intruder's initial compromise, to the time when a victim learns of a breach, is currently 205 days, as reported in our 2015 M-Trends report. This number is better than our 229 day count for 2013, and the 243 day count for 2012.[5] Unfortunately, it means that, for nearly 7 months after gaining initial entry, intruders are free to roam within victim networks.

What is the answer?

Before talking about solutions to digital risk, we need to define it. Always ask "Risk of what?" Are we talking about the risk of a teenager committing suicide due to "cyber bullying," or the risk of a retiree's 401k being emptied due to electronic theft, or the risk of a week-long power outage due to state-sponsored attack?

Step one is to define the risk, and step two is to measure progress by combining ways and means to achieve defined ends. This is exactly the role of strategic thinking, meaning the application of strategies, campaigns, tactics and tools to achieve organizational goals.

For example, a company may worry about the risk of losing intellectual property to foreign hackers. The board and management team works with the chief security officer (CSO) to define a company goal of minimizing loss due to digital intrusions. To accomplish the goal, they agree on a strategy of rapid incident detection and response. To achieve the strategy, the CSO develops a campaign to hunt for intruders in the company using network security monitoring (NSM) operations. To prosecute the campaign, the security team implements tactics to collect, analyze, escalate, and resolve intrusions based on NSM principles. Finally, the security team uses tools, or security software, to bring their tactics to life.[6]

[5] https://www.mandiant.com/resources/mandiant-reports/

[6] http://taosecurity.blogspot.com/search/label/strategy

To measure success, the security team should track the number of intrusions that occur per year, and the amount of time that elapses from the initial entry point to the time of discovery, and from the time of discovery to the removal of the threat. This strategic approach is the reason Mandiant calculates these metrics when helping breach victims.

Security professionals define Risk as the product of Threat, Vulnerability, and Cost, which is the impact of a security incident. We use a pseudo-equation where R = T x V x C. We're not trying to calculate a number. We're trying to show how Threat, Vulnerability, and Cost influence Risk. If any factor increases, Risk increases, and if any factor decreases, Risk decreases. We appear to live in an environment where Threat, Vulnerability, and Cost continue to rise, driving up Risk, but note that reducing any component -- Threat, Vulnerability, or Cost -- helps lower Risk.

Too often the more engineering-focused members of the security community fixate on Vulnerability. We hear of "game-changing technologies" promising to remove flaws, reduce attack surfaces, and so on. While I accept the need for more secure software, we must not neglect the role of reducing the Threat and the Cost they impose.

Law enforcement and counter-intelligence operations are the primary means by which we can mitigate the Threat. In an editorial for the Brookings Institution titled "Target Malware Kingpins," I asked "what makes more sense: expecting the two billion Internet users worldwide to adequately secure their personal information, or reducing the threat posed by the roughly 100 top-tier malware authors?"[7] Along those lines, I applaud the FBI's recent announcement of a $3 million bounty for information leading to the arrest of a Russian hacking suspect who stole more than $100 million since 2011.[8]

Reducing the Cost of security incidents takes somewhat more creative approaches. One step in progress is the "tokenization" of the payment card system, whereby strings of numbers, or "tokens," replace traditional credit card numbers. A second step would be eliminating the value of Social Security

[7] Richard Bejtlich, "Target Malware Kingpins," The Brookings Institution; http://www.brookings.edu/research/opinions/2015/02/02-cybersecurity-target-malware-kingpins-bejtlich

[8] http://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

numbers to identify thieves. I recommend reading the Electronic Privacy Information Center's suggestions on "effective SSN legislation" for policy changes.[9]

In brief, defenders win when they stop intruders from achieving their objectives. It's ideal to stop the adversary from entering the network, but that goal is increasingly difficult. If traditional defenses fail, you must quickly detect the intrusion, and respond to contain the adversary, before he steals, changes, or destroys the data or system under attack.

Finally, we must appreciate that the time to find and remove intruders is now. There is no point in planning for theoretical, future breaches until you know your own, current, security posture. If a company hired me to be their CSO, the first step I would take would be to hunt for intruders already in the network.

I look forward to your questions.

[9] https://epic.org/privacy/ssn/

Mr. MURPHY. Thank you.

Now, Dr. Shannon, you are recognized for 5 minutes.

TESTIMONY OF GREGORY SHANNON

Mr. SHANNON. Thank you. Thank you, Chairman Murphy, Ranking Member DeGette, and distinguished subcommittee members. I am honored to testify before you today on cyber threats and implications for the 21st century. I am Greg Shannon, the Chief Scientist for the CERT Division at the Software Engineering Institute, which is a DoD, FFRDC, operated by Carnegie Mellon University.

To sustain and expand our economy, consumers and businesses need to trust the cyber infrastructure ecosystem upon which commerce and innovation now depend. Those ecosystems must also thwart capable adversaries who seek to execute economy-disrupting cyber attacks. Today, in cyberspace, as noted before, there is no manner in which an entity, public or private, can fully protect itself without simultaneously eroding its own value. There are neither existing technologies nor any amount of money that would stop all serious cyber attacks, and allow for the efficient function of electronic commerce. We simply do not yet know how to do both.

As technologists, what are we to do? In the short term, we need to push for more and better measurement of outcomes, as noted earlier. Security successes as well as breaches. Collectively, if most everyone practices good cyber hygiene, we are unlikely to be undone by the weakest link, however, you cannot expect everyone to adopt a new idea without proof of efficacy, especially when implementation isn't free. The opportunity of measuring outcomes directly applies to two promising risk management frameworks, the NIST Cybersecurity Framework, and the Department of Energy's Cybersecurity Capability Maturity Model. Both of these frameworks are being measured for efficacy and will soon produce data telling us which practices matter. We need that feedback. The best-secured organizations continuously monitor how their performance correlates with their practices. Without meaningful feedback, the state-of-the-art cannot improve.

In the medium-term, we need to improve access to data, specifically for security and privacy innovation. Cyber solutions are only as good as the data they are created from. And currently, researchers and developers have limited access to data, resulting in subpar solutions and slower innovation. Sadly, just this morning, I listened to research results based on 15-year-old synthetic dataset with known serious limitations. Fortunately, I have also personally seen security innovation accelerated when scientists and engineers have access to good data; i.e., when modeling insider threats. If we can determine which subsets are essential for combatting those cyber threat, then less data would need to be shared and thereby possibly moderating privacy concerns.

In the long-term, we need a coordinated national strategy to sustainably build trust and thwart our cyber adversaries. For example, we need to eliminate the possibility that a single weakness can threaten the economy. Considering computational and human energy as a barrier, it is possible to create and operate a strategically advanced cyber infrastructure that would require adversaries to expend exceptional energy in order to pose serious cyber threats to our economy. Today it takes only modest computing and human energy to find and execute economy-threatening attacks, creating an environment that favors the adversary by orders of magnitude. Given the energy we already expend on security defenses, we can optimize our energy investments to create a more robust defense, and simultaneously apply recent research results and new technologies that makes the computational cost of finding and executing a compromise exceptionally high. In June, a DIMACS- and IEEE-sponsored workshop at Carnegie Mellon will discuss the technical foundations of this strategy. If we can create and operate a strategically advanced cyber infrastructure that requires adversaries to expend astronomical amounts of energy to find and execute economy-threatening attacks, then energy becomes the currency in which one traffics to protect or attack commerce around the world. Ultimately, access to energy could become a deterrent to economy-threatening cyber attacks.

Over the last 45 years, we have created the Internet and a modern evolving 21st century economy. Paradoxically, our own innovation and collective success have created today's trust and resiliency challenges. Nevertheless, I am optimistic that over the next 45 years, we will make our 21st century economy fully trustworthy and resilient.

Thank you.

[The prepared statement of Mr. Shannon follows:]

Hearing on "Cyber Threats and Implications for the 21st Century Economy"

Written Testimony of Gregory E. Shannon, Ph.D.

Chief Scientist for the CERT Division

Carnegie Mellon University

Before the Subcommittee on Oversight and Investigations

U.S. House of Representatives Committee on Energy and Commerce

Future Technologies for a Trustworthy and Resilient Cyber Economy

March 3, 2015

Chairman Murphy, Ranking Member DeGette, and members of the subcommittee, thank you for inviting me to testify on cyber threats and implications for the 21st Century.

My name is Greg Shannon, and I am the Chief Scientist for the CERT Division (www.cert.org) at the Carnegie Mellon University Software Engineering Institute where I lead efforts to sustain and broaden CERT's strategic research, development, and policy initiatives. I also chair the Cybersecurity Initiative for IEEE (www.ieee.org); my goal is to accelerate innovative research, development, and use of efficient cyber security and privacy technologies that protect commerce, innovation, and expression.

On behalf of Carnegie Mellon University and IEEE, I am honored to discuss future technologies for a trustworthy and resilient cyber economy.

Summary of Major Points

To sustain and expand our economy, consumers and businesses need to trust the cyber-infrastructure ecosystems upon which commerce and innovation now depend. Those ecosystems must also thwart capable adversaries who seek to execute economy-disrupting cyber-attacks.

Currently there is no manner in which an entity, public or private, can fully protect itself without simultaneously eroding its value. There are neither existing technologies nor any amount of money that would stop all serious cyber-attacks and allow for the efficient function of electronic commerce. We simply do not yet know how to do both of those together.

In the short term, we need to push for more and better measurement of outcomes. The best-secured organizations continuously monitor how their performance (breaches) correlates with their practices. Without meaningful feedback, organizations (and technologies) cannot improve. Furthermore, if we can determine which data subsets are essential to combating the cyber threat, then less data would need to be shared to productively handle cyber risks.

In the medium term, we need to improve access to data for security and privacy innovation. Science or technology are only as good as the data it is created from, and currently researchers and developers have limited access to data, resulting in sub-par solutions and slower innovation.

In the long-term, we need coordinated national strategies to sustainably build trust and thwart our cyber adversaries. For example, we need to eliminate the possibility that a single weakness can threaten the economy. Considering computational and human energy as a barrier, it's possible to create and operate a strategically-advantaged cyber infrastructure that requires adversaries to expend exceptional energy in order to pose serious cyber-threats to our economy.

Testimony

As we strive to grow our Nation's 21st century economy, we must expand trust of the cyber-infrastructure ecosystems used by both public and private users. Today, national and global commerce depends upon those critical cyber ecosystems, yet a multitude of threats exist across the spectrum from individuals to collective groups that seek to disrupt commerce through cyber-attacks. Maximum global economic advantage will come to those ecosystems that can best thwart increasingly sophisticated adversaries.

Currently there is no manner in which an entity, public or private, can be fully protected without simultaneously destroying its value. Today, there are neither the tools, technology, nor resources, to stop all serious cyber-attacks and allow for efficient function of electronic commerce. We simply do not yet know how to do both of those together, which makes enabling continued technology research and innovation essential.

Innovation

Merriam-Webster defines *innovation* as a new idea, device or method. While people often think of a novel device when they hear the word *innovation*, we must remember that it can also refer to innovative concepts in business models, policy, social interactions, education, etc.

In business, innovation brought the Freemium[1] model, a pricing strategy by which a basic product or service is provided free of charge, while money (premium) is charged for proprietary features. Innovation in social media delivered crowd sourcing and open source solutions. Disruptive policies such as the European Union's (EU) "Right to be Forgotten" have influenced and changed our world. Even the long-standing framework for Internet governance with ICANN

[1] See Anderson's book *Free*, published in 2016.

(Internet Corporation for Assigned Names and Numbers, the private sector, non-profit corporation created in 1998 to assume responsibility for administering IP addresses), IETF (Internet Engineering Task Force) and IAB (Internet Architecture Board) were truly innovative. Similarly, in education, we have distance learning, adaptive learning like CMU's OLI initiative[2], and immersive team virtual learning in CERT's STEPfwd platform.[3]

The bottom line is that when we discuss innovation we do not want to pigeonhole ourselves to only hardware and software. Instead, we need to expand our view to include that which will advance us from the status quo.

Technology Outlook for the Future

When discussing cyber security—past, present or future—it is important to understand the four mainstays of cyber technology and innovation: trust, people, efficiency, and measured outcomes. Innovation and the adoption of new technologies must take into account those four pillars.

The technologies I discuss later broadly facilitate these pillars and provide a sound basis for a trustworthy cyber infrastructure that thwarts successful attacks. First, I want to explore near-term, medium-term, and long-term technology research opportunities.

[2] http://oli.cmu.edu/get-to-know-oli/
[3] https://stepfwd.cert.org/

Near-Term Opportunity

In the current reality, individuals, businesses or national organizations cannot expect to prevent every serious cyber attack. Such entities must be aware, resilient, enabled, and capable to continue operations and meet their missions when disruption occurs. Organizational resiliency requires a structured approach to managing security risks, business continuity, and information technology operations within the context of business objectives. But without proof about which ideas, processes, or devices work, or in other words, return on investment (ROI), adoption rates of such approaches languish. Consequently, in the short term, we need to push for more and better measurement of outcomes to galvanize adoption rates.

It is not news that cyber connects us all: private and government, personal and business, entities and individuals. Collectively we're unlikely to be "undone" by the weakest link, if most everyone practices good cyber hygiene. However, you cannot expect everyone to adopt a new idea without proof of efficacy, especially when implementation rarely comes free. We, as a Research and Development (R&D) community, need to ensure innovation is scientifically and operationally validated and provide compelling return on investment metrics to incentivize adoption.

There are two working approaches we can use to set in motion a protocol of gathering feedback to produce meaningful metrics. The first, and most obvious, is the NIST Cybersecurity Framework (CSF). With incentives and a sound legal framework, organizations could begin to extract data, employ metrics and share those with both their peers and the Federal Government.

The second model is the Department of Energy's (DOE) successfully deployed Cybersecurity Capability Maturity Model (C2M2), which is a public-private partnership effort established as a result of the Administration's efforts to improve the electricity subsector cybersecurity capabilities. The C2M2, focused on the implementation and management of cybersecurity practices, helps organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity capabilities.

Moving forward, policymakers have the potential to enable progress in the science of cyber security with explicit guidance that policies, best practices, technologies, standards, products, and large-scale operational plans are scientifically and operationally validated and will produce valid, outcome-based, efficacy measurements. The best-secured organizations continuously monitor how their performance (breaches) correlates with their practices. Without meaningful feedback, organizations (and technologies) cannot improve.[4]

Medium-Term Opportunity

Medium-term goals must include access to data for research and development (R&D). Currently, the R&D community has limited access to data, resulting in sub-par solutions and stunted innovation. Information sharing is often seen as a defensive strategy; however, providing operationally relevant data to researchers and engineers accelerates innovation. I've personally seen such acceleration in sponsored research and the development of commercial technology.

Richer data needs to be shared with the research and development community — meaning not only incident data but also datasets that enable understanding of what "normal" resembles (in terms of network activity, user behavior, etc.). If situational awareness is to develop beyond simple indicators, researchers and developers need access to everyday data so that they can begin to recognize what datasets are important. If the research community were able to successfully

[4] A paper by Ericsson, asserts the need for meaningful feedback in order to become a capable expert. Consistent with current business research, I believe that the same applies to improving an organization's resilience.

determine which features in datasets were essential to combating the cyber threat, then in effect, over time less data would need to be shared to productively handle cyber risks.

It is imperative that policymakers include research in the information-sharing vernacular. To encourage unencumbered information sharing, of course, solid protection procedures need to be in place. This will likely require both legislative updates and policy changes, which must be done with the utmost consideration of privacy and civil liberties.

It is the Federal Government's role to generate situational awareness beyond what any private entity has the incentive to produce. But we must be mindful to not simply generate compliance-driven information while incentivizing minimal disclosure. Building trusted relationships with stakeholders becomes essential to avoiding limited information exchange and is fundamental to a successful response.

I realize additional information sharing tends to exacerbate an already contentious relationship between security and privacy. Security and privacy advocates often are at odds with one another in discussions of how security degrades privacy or privacy degrades security. This is an unhealthy condition, and our adversaries are exploiting it and degrading cyber space for us all. Privacy advocates contend without privacy there is no security. But given our ever more interconnected world, the loss of anonymity is unavoidable, and I believe that without security there is no privacy.

Long-term Opportunity

In the long term, our Nation needs a coordinated and integrated cyber security strategy to build trust between public and private entities and thwart our capable cyber adversaries. Cyber innovation and research need to address the threat in a more holistic manner. Currently, we have tools and solutions to address pieces of the cyber problem. Organizations have to filter hundreds of options to pick the few that fit within their budgets. At the same time, they have to hope that their choices will deflect the majority of attacks. Researchers and policymakers should work towards technologies and innovation that make cyber attacks exceptionally more complicated than exploiting a single weakness.

We all know that there is no silver bullet, but consider if we created a cybersecurity solution that could increase the trustworthiness of cyber infrastructure while simultaneously providing a significant and structured energy-based barrier to cyber attacks. Today, it takes only modest energy (computing and human) to find and execute economy-threatening attacks. This creates an environment that favors the adversary by orders of magnitude. Given the energy we already expend in security defenses (firewalls, anti-virus, intrusion detection systems, etc.) and data analysis of network and host behaviors, we could (1) optimize our (energy) investments to create a most robust defense, (2) utilize recent research and new technologies that make the computational cost of compromise exceptionally high, and (3) we could optimize the energy efficiencies and costs in each technology.

We believe that if we can create and operate a strategically advantaged cyber infrastructure that requires adversaries to expend astronomical amounts of energy to find and execute economy-threatening attacks, then energy becomes the currency in which one traffics to protect or attack commerce around the world. The kilowatt-hour unit of energy is well-defined, measurable, cannot be counterfeited, and has real value, thus making it an excellent form of symbolic currency—in this case the tender to employ or thwart cyber attacks.

Director of National Intelligence James Clapper told Congress on Feb. 26 that he is most worried about the moderate, iterative and constant barrage of cyber attacks on U.S. infrastructure that will "impose cumulative costs on U.S. economic competitiveness and national security." DNI Clapper's recent testimony on this "insidious trend" supports my belief that energy resourcing will be necessary and required as part of a comprehensive national security strategy to effectively thwart cyber invasions.

Such an energy-based obstruction to cyber threats would require us to first create more energy-efficient technologies to ensure operational cyber security and to establish valid assertions about the amount of energy required by adversaries to compromise the security. Finally, we would have to apply energy to the secure creation, operation and monitoring of cyber operations. With innovation for efficiency and our own national energy resources, only peers with similar resources are even strategically competitive.

This could be a game-changer and would certainly level the playing field. Requiring a greater expenditure of energy currency could also form a barrier to entry for smaller groups and individuals—eliminating foes before they start. Furthermore, embracing the "energy currency" would allow us to standardize and better measure how much we spend, or need to spend, on cyber security as well as force our adversaries, to include nation-states, to prioritize and even reduce the extent of attacks they are able to attempt. Ultimately, access to energy could become a deterrent to economy-threatening cyber attacks.

A DIMACS- and IEEE-sponsored workshop at Carnegie Mellon University in June[5] will explore the theoretical and technical foundations for this strategy.

[5] http://dimacs.rutgers.edu/Workshops/ESCAPE/announcement.html

Technologies to Watch

An excellent resource for understanding future cyber technologies is the IEEE Computer Society 2022 Report,[6] a survey of 23 technologies that could change the world by 2022. Notably, the first technology that this report addresses is security cross-cutting issues, Trust issues (i.e., privacy) are considered throughout the report.

I would like to draw attention to some of the key emerging technologies I believe will enable us to sustain cyber trust and impede cyber adversaries over the short-, medium-, and long-term.

Key Short-Term Technologies

- Risk modeling and management: the only viable strategy for dealing with limited resources, uncertain knowledge, and incomplete solutions
- Two-factor authentication: an effective and scalable technology with many variations
- Cyber intelligence analysis:[7] know and track adversaries on their specific objectives, techniques, and operations

Key Medium-Term Technologies

- Resilient trustworthy ecosystems: "app stores" for mobile phones, secure software updates, enterprise cloud computing services
- Efficient security & privacy architectures, design methods,[8] and development tool chains
- Cyber-relevant theory and models of humans (individuals and communities): Understand how/where the range of human behaviors can enhance/degrade security and privacy.

[6] http://www.computer.org/2022

[7] Information sharing is helpful, but it is not a panacea for the overall cyber threat.

[8] A first step in towards secure designs: Avoiding the Top 10 Software Security Design Flaws, http://cybersecurity.ieee.org/images/files/images/pdf/CybersecurityInitiative-online.pdf.

Key Long-Term Technologies

- Security- and privacy-preserving computing: fully secure encryption, private database queries, verified computation
- Proofs of correctness and searches for counter-examples (e.g., bugs, exploits): already used to verify device drivers and some protocols, and to find exploits in deployed code
- Quantum-secured communication: solves an important but narrow part of the problem: concerns about scalable deployment

Education and workforce development

Both the public and private sectors must have an agile and prepared workforce to deal with the cyber environment and should to be able to train them in a cost effective and scalable manner. Responding to critical cyber events requires technical knowledge and skills, decision-making abilities, and effective coordination—all while moving rapidly.

Institutions like Carnegie Mellon University, with its numerous degrees and professional training programs as well as its technologies rooted in the science of learning like OLI, and the IEEE, with its Cybersecurity Initiative,[9] are well suited to ensure that we have the workforce trained and equipped to handle future cyber threats.

Keeping the workforce up to date is a major challenge given the rapidly changing and dynamic nature of cybersecurity. Curriculum creation needs to be an agile process, with the capability to easily add and modify material. Likewise, education delivery needs to emphasize simulations and scenarios. Currently the most common workforce development training solution is traditional classroom training. While easy to implement, the classroom training solution is not

[9] http://cybersecurity.ieee.org/

adequate for providing effective, large-scale training to a technical workforce. It is also not optimal for training the workforce in a rapidly changing field such as cybersecurity.

The best way to prepare the workforce is to provide practice opportunities under realistic conditions using interactive simulations. Participants across multiple locations are working together in these simulations, to analyze and respond to threats and attacks. This training needs to be delivered on a platform that safely mimics how the internet would respond to stress and exposes participants to real-world, job-relevant scenarios, events, and activities.

CERT's workforce development research focuses on the problems of time, efficiency, scale, and cost. Our researchers, engineers, and subject matter experts search for innovative ways to compress the time it takes to build cyber expertise and to amplify that expertise across a globally distributed workforce. We perform this important research and development to determine how expert content and custom delivery platforms can be used to facilitate efficient transference of knowledge and skills to the cyber workforce.

We have developed custom training platforms that support a range of learning methodologies from traditional, static learning content all the way to interactive, hands-on cybersecurity training scenarios. We provide two comprehensive solutions, STEPfwd[10] and FedVTE, which provide cybersecurity professionals a rich resource of training and skill development important to their work. We facilitate cyber training exercises to apply skills in environments that simulate real-world infrastructures and attacks. Multiple installations of the same exercise can be deployed simultaneously to accommodate a large number of participants.

[10] https://stepfwd.cert.org/

Conclusion

Over the last 45 years we've created the Internet and a modern, evolving 21st century economy. The trust and resiliency challenges have been created by our collective innovation and success. Over the next 45 years, I believe that we can sustain this new economy by making it fully trustworthy and resilient.

Institution Backgrounds

Founded in 1900 and located in Pittsburgh, Pennsylvania, Carnegie Mellon University is the youngest of the top 25 universities in the United States and consistently ranks among the top U.S. universities in computer engineering, computer science, the arts, and public policy for information technology. A global institution with campuses in Silicon Valley, Qatar, Portugal, Australia, Rwanda, and China, Carnegie Mellon is the birthplace of research on artificial intelligence, home to the first university robotics institute, and the first graduate program in entertainment technology. It is among the top U.S. academic institutions in spinning out companies, launching over 75 companies in just the past two years. By any metric, CMU spins out more companies per dollar of federal research funding spent. Recognized as a leading force in the transformation of the Pittsburgh economy, it is credited with helping to attract Google, IBM, Apple, General Dynamics, Network Appliances, Disney Research, Caterpillar and Uber to southwestern Pennsylvania. Over 80 faculty are engaged in life sciences related work that ranges from the development of assistive heart devices to cognitive neuropsychology.

The CERT Division is part of the Carnegie Mellon University Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) sponsored by the Department of Defense. The SEI is headquartered in Pittsburgh, Pennsylvania, with facilities in

Arlington, Virginia (www.sei.cmu.edu). As the birthplace of modern cyber emergency response capabilities in 1988, the CERT Division (www.cert.org) researches, develops, promotes, and operates technology and systems management practices to resist attacks on networked systems, limit damage, restore continuity of critical systems services, and investigate methods and root causes. CERT works both to mitigate cyber risks and to facilitate local, national, and international cyber incident responses. Over the past 26 years, CERT has led efforts to establish more than 110 computer security incident response teams (CSIRTs) around the world, including the Department of Homeland Security (DHS) US-CERT.

With more than 400,000 members in over 160 countries, IEEE— founded as the Institute of Electrical and Electronics Engineers, Inc.—is the world's largest organization for technical professionals, and a leading educational and scientific association for the advancement of technology. The IEEE Computer Society is the trusted information, networking, and career-development source for a global community of technology leaders that includes researchers, educators, software engineers, IT professionals, employers, and students.

Mr. MURPHY. I thank all the panelists for their testimony. And now I am going to recognize myself for 5 minutes for questions.

So we have heard a lot about the nature of cyber threats and cybersecurity. We heard it is very asymmetric, it favors those who wish to misbehave in cyberspace, and defenders have to spend a great deal of time and money and very complex systems all at once. So this is a question for any of you. Can this asymmetric imbalance be corrected to favor defenders instead of attackers? Any of you want to weigh in on that? Dr. Lin?

Mr. LIN. Sure. I don't know if it will ever be able to favor the defense, but you can certainly make it a lot harder for the attackers. I think there is no question about that. I think all of my colleagues here basically said that, that we can do a much better job than we are doing now. For example, there are known technologies and known procedures, and so on, that we can deploy that will increase security, but we just don't use them, for a variety of reasons.

Mr. MURPHY. Anyone else want to weigh in on that before I go on to my next question?

Mr. BEJTLICH. Sir, just briefly, I could give you a tactical answer. The iPhone is an example of a more secure technology that people love, and the reason is is Apple has an App Store that it polices closely; it is very difficult to get something malicious in there. So when you look at vulnerabilities on phones, there is a fraction of what is on Android as compared to Apple because Android is much more open, Apple is more closed. Now, if you want to be able to run whatever you want on your iPhone, you lose that, but it is more secure.

At a more strategic level though, we have to realize that it does take effort for intruders to get their objectives done. It is not like a silver bullet attack where they press a button and the end of the world happens. We have seen intruders take days, weeks, even months, to get to the data that they need. So sometimes it is a question of your perspective as well.

Mr. MURPHY. So let me jump onto that and, Dr. Shannon, maybe you could follow this. So are there opportunities that we can increase the cost for the bad guys in doing business, so we can do some technical things, which you just described Apple does, but are there other things, perhaps legal or technological solutions that we can take steps on?

Mr. SHANNON. At the technological level, as I point out in my written testimony, there are some long-term research and development opportunities. Technology that is coming to fruition is becoming practical. Essentially, it makes the computations similar to— if you were to break the computation, it would be similar to breaking encryption. And so the goal is to make it so that database queries, remote computation in the Cloud, is just as difficult of disrupting and compromising as it is encryption. And these typically are encryption-based technologies, and hence, my comments about high energy, that the amount of energy it would take an adversary to compromise those systems, or to find a way to thwart those systems, would be comparable to breaking encryption.

Mr. MURPHY. Let me jump onto a different part here. So let us talk about the Internet of things. We are going to have all these things controlling parts of our lives, from running our dishwasher to opening and closing garage doors, turning the heat on and off, tracking where we are, finding where our kids are, is it possible to keep pace with these threats, and let alone increase the cost of attackers, as we are talking about here, to malicious actors? Dr. Lin, can you weigh in on that?

Mr. LIN. Is it possible to do better than they are likely to do? Sure, but the problem is that getting stuff out first to market is an effort-intensive thing, and you don't want to put in effort to focus on security before you can get to market. And they do this for perfectly reasonable economic reasons, but it is very hard to get people to focus on cybersecurity in the absence of some sort of mandate before they have gotten the product out.

Mr. MURPHY. So that becomes something we can work on in Congress.

Mr. BEJTLICH. Sir, there is an opportunity here, and that is, with traditional security, you have been relying on a person to secure their computer. Someone who is not an expert, someone who is just a user. With a vendor, you have a centralized place where you could apply some pressure of a variety of means to get them to have their act together as far as, for example, securing my refrigerator. There is nothing I can really do to my refrigerator. It is not like my PC. So you can apply some pressure on the vendor to make sure that they have their act together.

Mr. MURPHY. OK. Let me ask one more question in my brief amount of time. Dr. Shannon, you referred to the importance of trust and trustworthy things. We want to be able to trust so many things that we are involved, with interstate commerce, with energy, telecommunications, all the things within the jurisdiction of this committee. So let me go back here, if we were to redesign, if the Internet was starting up today, how would we design it differently to take care to have that trust, still have something that is accessible, but is secure?

Mr. SHANNON. A big part of it is to look at the ecosystem that actually creates the components for the environment, the software, the hardware. Part of the challenge is that there is a very large shared base, and those systems have been created in an insecure manner. And so it provides ample opportunities for adversaries to work their way into, and they really create the opportunity to steal the private data and to bring down a banking site, or whatever. So that is where the real opportunity is if you designed it properly from the beginning.

Mr. MURPHY. Thank you.

Ms. DeGette, you are recognized for 5 minutes. My time is up.

Ms. DEGETTE. Thanks, Mr. Chairman. As I mentioned in my opening statement, the Federal Government and also private businesses have been targeted by cybercriminals, and I talked about Target, I talked about Home Depot, JP Morgan Chase, the health insurer Anthem. From the Federal Government side, also we have had substantial attacks. In July of 2013, there were hackers who stole social security numbers and other information from over 100,000 employees at the Department of Energy, for just one example.

So, Mr. Bejtlich, I heard a number that seems high, but if you add all these together, the number I heard is that over 100 million Americans could potentially be at risk from these cyber attacks. Does that number sound plausible to you?

Mr. BEJTLICH. Yes, just given the Anthem hack alone, close to 80 million records including social security numbers. So you get to 100 million pretty quickly.

Ms. DEGETTE. Yes. And so typically what companies do is they tell people they can have a year of free credit monitoring if they have had their data stolen. Do you think that is sufficient, or do we need to explore additional remedies?

Mr. BEJTLICH. I concur that that is not sufficient. I don't want to blame the victims in this case, but I was personally affected by the Anthem hack, as was my family, so the ability to recover from that doesn't exist in our system. It does exist for something like a credit card number. We have all had credit cards stolen and not suffered that much damage, but it is a whole other ballgame when you are dealing with social security numbers and other data.

Ms. DEGETTE. And do you have some ideas what we could do, aside from giving people free credit monitoring?

Mr. BEJTLICH. Well, I think the first thing is to go through an exercise that says what data exists, and what happens when that data is an intruder's hands, in a criminal's hands, what can be done with that data. And if there is no friction from having the data to opening a new line of credit, getting a mortgage, whatever it is, we need to introduce some friction there, whether it is some type of physical agreement that has to be passed through the mail, or something that makes it more difficult for the intruder, and allows the victim to know something is going on here and not just wait until you have gotten an adverse credit report.

Ms. DEGETTE. Yes, and is that something that you think Congress should be involved in?

Mr. BEJTLICH. It is not my place to say what you should do, I believe, but I do think we need more industries thinking in terms of what happens to data post-breach, because I agree with your statement that we are either post-breach or pre-breach for most organizations.

Ms. DEGETTE. Right. Right, and I mean what you are saying is, if somebody hasn't had their data stolen, it is likely that they will have their data stolen, correct?

Mr. BEJTLICH. Some data, yes, of some type. As we have all heard, more of our data is out there.

Ms. DEGETTE. So do you think it might make sense to let consumers lock their credit down with credit agencies? Do you think that might be one solution?

Mr. BEJTLICH. Ma'am, I am not an expert in the credit system, although my understanding of the current system is that that is not an easy proposition. I think we may need to look at something that would allow that to happen, for example, I have young children, there is no reason for them to have any credit taken out in their name until there is some type of formal approval.

Ms. DEGETTE. And that was my next question is that would be one thing that would be easy to do. Is there some other way we can protect children from early identity theft?

Mr. BEJTLICH. I do know that the act of credit monitoring, and this has come out through the disclosures that I have received as a victim of some of these cases, the act of trying to do credit monitoring, or to do a credit check for a child makes them more likely, or makes it easier for an intruder to use their identity. So that seems like a situation that needs to be changed.

Ms. DEGETTE. So I have one more question for anybody who wants to answer it. My staff here recently—you met with Sysco?

VOICE. Citigroup.

Ms. DEGETTE. Citigroup? Citigroup. And they did a test on their own systems, and what they found was that these breaches were actually interactive. So they could breach one machine and then it would actually morph when it went to the next machine. It would actually change. And so that is the sophistication they are getting now. What can we do to start trying to protect against those sorts of breaches? Anybody.

Mr. SHANNON. Well, the cyber threat analysis is a key part of that in terms of being able to track an adversary, and track their TTPs, their tools, techniques and procedures, so that once you realize there is a breach, you realize what the next step for that adversary might be. And it is about using the cyber intelligence——

Ms. DEGETTE. Do we have the ability to do that now?

Mr. SHANNON. There are commercial organizations that actually do that. I believe that is part of what you guys do for your bread and butter.

Mr. LIN. The problem that you have described is what is known as a perimeter defense, and once you have breached the perimeter of an organization, you can do anything you want inside. Most organizations believe that they just erect a big enough of perimeter on the outside and they are safe, but they are not. And so organizations have to learn to practice and operate as though they had already been penetrated, and getting them to do that is a tough thing to do.

Ms. DEGETTE. Thank you.

Thank you, Mr. Chairman.

Mr. MURPHY. Thank you. They have called a vote, early as it is. So what we are going to—no, I guess it is on time. So what we are going to do is take a break. Don't go far because as soon as Members come back—I know Mr. McKinley ran so he will beat me back, so we can just continue on as soon as we get back here and have a chair. So don't wonder far, we will be right back. Thank you.

[Recess.]

Mr. MCKINLEY [presiding]. Now that we have some balance here, we can continue. And so we will continue the hearing. I believe I am the next questioner. So thank you very much for your patience on that, and now that we have a balanced panel, we can continue.

I am trying to follow some of the hyperbolae that goes on in Washington often about cybersecurity, terrorism, debt, climate change, I was interested in the last few days the—Lee Hamilton with the 9/11 Commission came out and said the biggest threat facing America is not ISIS, but cyber attacks. The FBI director said it is the greatest threat to national security. And the director of national intelligence, Clapper, said that the online assaults undermine U.S. national security.

Do you agree that that is one of our biggest threats if not the biggest threat that we face is the issue we are talking about here today? Each of you, just kind of a yes or no.

Mr. SHANNON. It is clearly a big threat. I think given that many other threats will result in direct loss of life, I think in the cyber arena it is pretty hard to make a compelling case based on experience to date. Is the potential there? Absolutely, but it is not, thank God, it hasn't manifested itself on a regular basis like it has in other areas.

Mr. BEJTLICH. Sir, I tend to think in terms of the actor, so cyber is a vector and a target, but at the end of the day, there is someone behind it, whether we are talking about the Russians or someone else, and I think that is why DNI Clapper elevated the Russian threat as above the China threat right now. The Russian threat is seen as more acute. It is linked to geopolitical events. It could be seen as a potential response to activity that is going on in Ukraine, whereas the activity from China is more stealing secrets and it is more of a chronic issue. So I tend to think in terms of who is it that we worry about, and less the way that they are going to do it.

Mr. MCKINLEY. OK. Dr. Lin?

Mr. LIN. I would agree with my two colleagues here, that it is one of the biggest threats. I would have a hard time thinking that it is worse than a nuclear weapon going off——

Mr. MCKINLEY. Sure.

Mr. LIN [continuing]. Improvised nuclear weapon going off, you know. I——

Mr. MCKINLEY. But if I could just continue with that because if it is a threat, and I think of small businesses, the Mildred Schmidt who lives next door to you, lives next door to me, she has no idea that she has been hacked, and they are getting into her information. I think if small companies—like my former company, that we did business with the Federal Government, and people could hack into my computer, and by virtue of that, get into the Federal computers. So we know it is out there. But what I did not like was, I guess it was, Mr. Bejtlich, something in your testimony, you said it may take 7 months before we know they are in there. This thing is just so broad, are we spending too much attention trying to focus on prevention and keeping actors out, or is there a better way to address this, because we seem like we may be shortening the time frame. Is this the best thing we should be doing?

Mr. SHANNON. Yes, that is certainly a concern. I mean we want to be able to build better infrastructure. You know, I am part of the Software Engineering Institute, part of our goal is to develop better methodologies for creating software assurance, and part of the challenges, as we were discussing during the break, is that the libraries that are out there that developers use, there are 15 million C programmers in the world, and they all go to places like GitHub and other open-source repositories to get a lot of their code, or to look at the code to see how it is done. And those codes haven't been hardened.

Mr. MCKINLEY. But Doctor, how do we deal with the small businesses that can't afford to build in all the software protection? How do we deal with that?

Mr. SHANNON. You want to provide a national asset where they can go to and get that as a given. If you provide repositories where there are already pre-hardened components, the developers would be using that if they are going to actually do some development. That——

Mr. MCKINLEY. Well——

Mr. SHANNON [continuing]. Is part of the benefit of ecosystems like IOS. Developers go there and they already know that they are using components that have been tested and approved.

Mr. MCKINLEY. Tested, OK.

Mr. BEJTLICH. I think insurance——

Mr. MCKINLEY. Mr. Bejtlich, it looks like you—OK, you wanted to say something?

Mr. BEJTLICH. Sorry, sir. I think insurance is also going to play a much greater role here. It is important to think in terms of—cyber is unique in some senses but in other cases it is not. So there are plenty of other real-world elements we can bring to bear on this, and insurance would be one of them. There is no reason for your small business to go out of business because of a hack if you can buy a policy that would help you recover from that.

Mr. MCKINLEY. Dr. Lin?

Mr. LIN. And I would say that there is a role for a single one-stop shopping for help if you have a computer security problem, that it would be helpful if your small business owner could know who to call. The problem with something like that is that what is going on in this person's computer is a very individual thing and there are going to be problems in responding, but at least people should be able to get help, and right now there isn't any good way to do that.

Mr. MCKINLEY. OK. So my time has run out on that, but thank you very much for that. I hope we can pursue that a little bit further.

Now, who do we have next? Our chairman is back.

Mrs. Blackburn, 5 minutes.

Mrs. BLACKBURN. Thank you, sir. I appreciate that, and I appreciate the patience that you all are showing by hanging with us as we are back and forth to the floor and different things.

Let me pick up right where Mr. McKinley left off. And as I said in my opening, that when you look at cyberspace, it is a place now where our information actually resides. Our virtual you lives there. And what we hear from constituents is how do I protect this, why can't they do something to make this safer? As my colleagues have heard me repeatedly say, there is nothing that women hate more than a peeping Tom, and they don't like them looking at their networks and their pictures and their photos and their passwords, and things of this nature, and the way they feel that violation is something that we hear about. So what I would like to hear from you all, and, Dr. Lin, you just alluded to this, when you said people want to know where to get help. So what do you see as a group of best practices that should be there for companies and their virtual space, whether they are a click business or a brick and mortar business, and then talk a little bit about B to C, and how businesses deal with consumers and inform and educate them as to what they are doing to make that virtual marketplace, and prohibit and incursions in cyber.

So let us start and just go down the line. We have 3 minutes, and I would like about 30 seconds from each of you on it.

Mr. LIN. One thing that businesses can do with respect to the consumers is to be more transparent about the ways in which they protect data and are willing to use it. Many companies are less than fully transparent in the ways in which they——

Mrs. BLACKBURN. So how they are crunching the data——

Mr. LIN. That is correct.

Mrs. BLACKBURN [continuing]. And what they are pulling from it, and go ahead and get permissions on the frontend.

Mr. LIN. Well, that is right, and to be fully disclosive about what they are actually going to——

Mrs. BLACKBURN. OK.

Mr. LIN [continuing]. What they could do with it.

Mrs. BLACKBURN. OK.

Mr. BEJTLICH. I would like to hear about the steps they take to protect data. Lots of times you hear, well, we can't talk about that because it will show too much to the adversary. I really don't believe that. I would like to know, for example, that my bank has an incident response team, that they exercise at regular intervals, they are staffed with these people that you may have heard of in the press. That, to me, would give me some comfort that they are taking that seriously.

Mrs. BLACKBURN. OK.

Mr. SHANNON. I think, actually, the marketplace has an opportunity to make this decision. I have seen some startups coming out that are promoting security higher to the users. And so if the company can indicate we are making things maybe a little more inconvenient for you, but it also makes it extremely more inconvenient for the hacker.

Mrs. BLACKBURN. Dr. Shannon, why do you think companies have not done that?

Mr. SHANNON. Well, because they see it as an impediment to their profit loss, they want to retain users, they want to make their services easy to use, and so they haven't been forced to, essentially, admit that——

Mrs. BLACKBURN. But then their customers become very angry——

Mr. SHANNON. That is correct.

Mrs. BLACKBURN [continuing]. When there is an incursion.

Let me—and it is Mr. Bejtlich, right? Am I saying that right?

Mr. BEJTLICH. Bejtlich. Thank you.

Mrs. BLACKBURN. Bejtlich. OK. I am close. That works. OK, let us see, Mandiant's M-trends 2015 report, something that caught my eye there was that you could have some malicious activity and a malicious actor on your system for 205 days. That was the average before it was discovered. And I found this so interesting because we had a company in my district there around Nashville that had a major breach this year, and the amount of time that the bad actor was on the system and then moved the information to a different system before they exported it and left——

Mr. BEJTLICH. Right.

Mrs. BLACKBURN [continuing]. The country with it. So do you concur with that 205 days, or is there a different—I know you all do a lot of remediation work, so——

Mr. BEJTLICH. Right. That is absolutely our number. That is based——

Mrs. BLACKBURN. OK.

Mr. BEJTLICH [continuing]. On our consulting work from last year. It is down from the year before which—we are moving in the right direction, but 7 months is still way too high.

Mrs. BLACKBURN. I agree with you.

And with that, I yield back. Thank you, Mr. Chairman.

Mr. MURPHY. Now recognize Mr. Collins for 5 minutes.

Mr. COLLINS. Thank you, Mr. Chairman. I want to thank you for coming in today to testify. The last Congress, I was the subcommittee chairman of Health and Technology on small business. I had a hearing on cybersecurity, and I don't think we can say this too often to small business, there is a threat to them, there is a threat to their very existence. And so maybe today we could just, Mr. Bejtlich, continue this discussion more as a PR to small business.

What I found was most small businesses are naïve to the threat. They operate under, "it won't happen to me." They are going to go after Target or Citibank or someone, they are not coming after my small business, which, in fact, and maybe you could expand on this, I think many of these folks see small businesses as the easy way into bigger companies. If they are a supplier to General Electric, if they are a supplier to a big company, an attacker can get into that small supplier and work through their connection to get through the supply chain, so to speak. But what we found was the staggering percentage of businesses that are out of business within 12 months of a data breach. It threatens their very existence because as, and you can expand on this really as well, if someone gets into their employee information, they have to provide credit insurance for that employee for some extended period of time, and that it out of their pocket, but also if a big corporation finds that that supplier was the access point, guess what, that big company is not going to buy from that supplier. If the customers find out, as we have seen, their data has been breached, they are not going to shop at that store.

So we are trying to say, and alert to small business—most of them don't have security policies, cybersecurity policies, they are sloppy with passwords, and they are just begging to be the target. So I don't know if you would want to just expand on a little bit of what I just said to—the warning to small businesses——

Mr. BEJTLICH. Sure.

Mr. COLLINS [continuing]. It can happen to you, and if it does——

Mr. BEJTLICH. I totally agree. The thing you should do as a small business is to say, first, what do we have that somebody else wants. That includes data as well as the money itself. I mean we have seen cases where ACH transfers of money just straight out the door and that is it, but it is also what data do we have, and what would be the consequences if that data were stolen. And then you have to go through the exercises of, well, how would that happen? Does it only take, say, an e-mail from the CEO that looks fake, that authorizes the money to be transferred out of our account. We have seen that happen as well. And once you figure out, OK, what do we have, what could happen to it, now you want to introduce friction into that system that would not make it easy for an intruder to carry that out. It could be something as simple as you have an email address, and if that single email is taken over by a bad guy, they could reset all your passwords, they could take over your bank account, so you want to make sure what are we doing to protect that.

A lot of this is just sort of thinking this through, just as you would estate planning or that sort of thing.

Mr. COLLINS. You would think it is commonsense, but it is not where you are worried about getting an order, getting it shipped, paying your bills, and it is just the thought that it can't happen to me. We have found so many companies, they don't even have a basic policy on passwords where many people use the same password at 100 different Internet sites. That way, they only have to remember one. But then these folks will get into that one, and then in a very short period of time, they can bounce that password into any number of other sites, and low and behold it hits. And the next thing you know, they are into that small business. They don't know it, as you pointed out. They are either taking their money, but worse yet, they are stealing customer information, IP, they are accessing the vendors and other customers. So to me, it starts with, you have to understand it can happen to you, number two, have a basic policy. We even published, when I was on the Small Business Committee, some dos and don'ts and the like, and just as an alert to small businesses who think it is only big companies. So you are confirming that small businesses are very much a target of the cyber——

Mr. BEJTLICH. Yes, sir. And I would add, talk to your bank and find out what can a bank do to tell you if something suspicious is happening. What is their policy, could they give you an alert of some kind, could you ask for a phone verification, an in-person verification. Put this friction in place so that it is not easy for a bad guy to steal all your money.

Mr. COLLINS. Yes, because they are out there.

Mr. BEJTLICH. That is right.

Mr. COLLINS. Thank you, Mr. Chairman. I yield back.

Mr. MURPHY. Gentleman yields back.

Now recognize Mr. Green of Texas for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. And I want to thank our witnesses. I apologize for goings and comings of the members because we had votes today. I guess for this hearing, the good news is that Homeland Security will stay in business.

But as we all know, last month, with the health insurer, Anthem, disclosed a significant breach of up to 80 million of its customers and employees. It is my understanding that the breach does not involve any credit or banking information, nor that there is evidence at this time that any medical information was obtained. While I appreciate the steps Anthem has taken to make it right with their customers, I do have some general questions on cybersecurity in the healthcare sector.

Dr. Shannon, is there any reason to believe that the healthcare industry is more vulnerable than other sectors to these type of data breaches, and do we have any reason to believe that the health sector is underinvesting in cybersecurity protections?

Mr. SHANNON. No, I think with the HIPAA Act that that has pretty much incented them to making investments.

Mr. GREEN. Which—that was in 1996, so——

Mr. SHANNON. Well, and that is really what has driven a lot of the cybersecurity thinking in that sector for the last 15 years. So I think similar to other organizations, they are investing. Fortunately, they are typically large organizations, so they often have resources and can—it is not quite the small business challenge that——

Mr. GREEN. Yes.

Mr. SHANNON [continuing]. We just heard.

Mr. GREEN. OK. Mr. Bejtlich?

Mr. BEJTLICH. Healthcare is definitely a target. They are not as well defended as the top tier. The top tier tends to be the defense companies and the financial sector. So yes, there is definitely an issue there.

Mr. GREEN. OK. Mr. Bejtlich, a different question. Is the health sector a particularly attractive target to hackers seeking to sell that personally identifiable information in the black market because, even though they didn't get maybe medical records, but they get social security numbers and everything else. Is that——

Mr. BEJTLICH. Yes, and one way, sir, we can measure that is how much does that sort of information sell for? You can get credit cards from $1 to $10, maybe a little bit more for an Amex or something like that, but if you are looking at a healthcare record with a social security number and such, you are looking at $300 perhaps. And so clearly, that information is more valuable.

Mr. GREEN. Who are the potential buyers for that kind of information?

Mr. BEJTLICH. It is not something we spend a lot of time on at Mandiant FireEye, although there are Eastern European criminal groups that apparently want to trade in that. I don't know if they are trading it in in bulk or individually. There is some thought that they trade for that information because it is so durable. You can change your credit card, you can't change a social security number.

Mr. GREEN. OK. Could stolen medical data be used to falsely bill for medical services, such as Medicaid or Medicare?

Mr. BEJTLICH. That is not an area that we work, but I have heard of that, yes.

Mr. GREEN. OK. I thank you. I would like to move the issue of notification of the patients in the event of a breach of medical information. Under current law, healthcare entities must provide notification of breaches of unsecured protected health information. Health information is considered unsecured essentially if it is not encrypted. Covered entities must notify affected individuals of a breach of unsecured protected health information within 60 days following the discovery of the breach. I think it is important to note that healthcare entities and medical information are already governed by a set of federal guidelines. I would like to ask all three panelists an open question about applying these standards. First, if you have 60 days to notify them, the cat is already out the door, it seems like, if you have that much time. Are there some basic standards such as encryption of certain data, or breach notification standards, that we may want to consider adopting as part of a federal cybersecurity guideline or national standard?

Mr. LIN. One——

Mr. SHANNON. One—go ahead.

Mr. LIN. One can certainly imagine mandates, well, encouragement for healthcare companies to protect their data. Internally, for example, you can do encryption of data even when it is within your system.

Mr. GREEN. Yes.

Mr. LIN. Theft of laptops has historically been an important vector where people steal information. If you encrypt the data on the laptop, it is a good thing. I caution that encryption is a costly—not costly, but I mean it is great—that results in greater inconvenience for the companies, and so they are going to complain about such mandates.

Mr. SHANNON. One of the challenges with regulations is that it encourages a compliance mentality, and I think we would all agree that compliance mentalities do not usually improve security dramatically. That is why I would encourage the healthcare industry to look at the NIST Cybersecurity Framework as a basis for managing cybersecurity risks, as opposed to compliance as the real driver.

Mr. BEJTLICH. And I would briefly like to encourage those companies to first look to see if there are intruders already in your network, and secondly, to have someone test to see how difficult it is for them to get into your network, and then act on the results.

Mr. GREEN. OK. Thank you, Mr. Chairman. I yield back my time.

Mr. MURPHY. Thank you.

I know Mr. Mullin was on his way, but that may be it for the hearing. I really want to thank you. This is valuable information, and let me—do you have any final closing comments you want to make? First, Ms. DeGette.

Ms. DEGETTE. I think this is a good scene-setter for our future hearings, and I would just advise the—I know, Mr. Chairman, you will let people know that people might give written questions after this hearing. I know some of the Members on our side wanted to come back but they got stuck after the vote. So we appreciate your wisdom and you may have some written questions coming after this. Thank you. I yield back.

Mr. MURPHY. I thank you. And we will probably be calling upon your expertise. We thank you for taking time out, and for the caliber of this. We will be dealing with a number of serious issues in this committee. Dr. Burgess is on this subcommittee, he is also chairman of Commerce, Manufacturing, and Trade legislation risk committee, but also Mr. Walden is chairman of Communications and Technology, we have the Energy and Power Committee, they have the Health and Subcommittee, all of these things here will be dealing with some multiple levels. The way I like to review it is we have the dot-coms, the dot-mils, the dot-govs, the dot-orgs, the dot-edus. Have I left anything out? We have to do what the committee—the dot-Greens, the dot-Tex, whatever. But thank you so much for this. To that end, I ask unanimous consent that the Members' written opening statements be introduced into the record. So without objection, the documents will be entered into the record, including the one that you have, Dr. Lin.

And in conclusion, I want to thank all the witnesses and Members that participated in today's hearing. I remind Members they have 10 business days to submit questions to the record, and I ask that all witnesses agree to respond promptly to the questions. Thank you so much.

And with that, this committee is adjourned.

[Whereupon, at 3:41 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Last December, in the wake of the Sony breach, I announced that the committee would hold a series of hearings to examine the growing cyber threats to electronic commerce and the American economy. That effort is now underway.

So much of our daily existence depends on the Internet and information technologies that collectively comprise cyberspace. These technologies have brought tremendous convenience, opportunity, and prosperity to the United States and nations across the globe. They inspire innovation, freedom of expression, and international and cultural engagement. They continue to revolutionize the way we communicate, learn, innovate, govern, and interact with the world around us.

At the same time, cyberspace has introduced us to new challenges. For the same reason a business in Michigan can reach customers across the globe, an unknown bad actor can target that business' intellectual property, customer information, or operations. The consequences and costs of such a breach can be significant, yet the costs of launching the attack, and consequences for failure, are minimal. As a result, the incentives strongly favor the bad guys—and they will keep coming, keep evolving—while the good guys struggle to keep pace.

As more of our lives are entrusted to cyberspace, the threats will continue to grow. Already, barely a day goes by where we do not learn of a new breach or potential vulnerability. With everything from health records to toasters increasingly integrated into cyberspace, the challenge can appear daunting.

We will hear today that there is no easy solution to the cyber threat. It exists for the same fundamental reasons that the Internet, information technology, and cyberspace provide benefit to society—that is, that the Internet remains an open system accessible to anyone who wants access. This may sound frightening or overwhelming, but I suggest it presents an opportunity. Today we have an opportunity to reframe our understanding of this challenge, to develop a level of context and perspective that so often gets lost in debates over specific incidents, policy issues, or legislation.

I encourage my colleagues to embrace this opportunity. Let's learn from this discussion so we can approach cybersecurity with fresh perspective and a common understanding of the challenges it presents.

Cyberspace has been, and will continue to be, an engine of economic, social, and cultural opportunity. We need to understand the nature and scope of the threat to the security of information in cyberspace, and develop an understanding of how to address these threats without jeopardizing the fundamental benefits that cyberspace provides.

This hearing is just the beginning as our work continues.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

February 27, 2015

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on "Understanding the Cyber Threat and Implications for the 21st Century Economy"

I. INTRODUCTION

On Tuesday March 3, 2015, at 2:00 p.m. in 2322 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled "Understanding the Cyber Threat and Implications for the 21st Century Economy." This will be the first in a series of hearings focused on cyberspace, the Internet, and the challenges and opportunities that they present. Cyberspace has become the backbone and engine of the 21st century economy, and recent high-profile information security breaches have raised awareness of the vulnerabilities and risks facing cyberspace. With this hearing series, the Subcommittee seeks to expand the discussion surrounding these issues to examine the broader implications for businesses and consumers in today's 21st century economy. This initial hearing will provide an overview of the issue, focusing on the history, evolution, and future of cybersecurity.

II. WITNESSES

- Herbert Lin, Senior Research Scholar at the Center for International Security and Cooperation and Senior Fellow at the Hoover Institution, Stanford University;
- Richard Bejtlich, Chief Security Strategist, FireEye, Incorporated; and,
- Gregory Shannon, Chief Scientist, CERT Program, the Software Engineering Institute, Carnegie Mellon University.

III. SUMMARY

Over the past two-and-a-half decades, society has become increasingly dependent on the Internet. Governments use it to interact with their citizens. Businesses use it to develop global markets. Individuals use it to connect with each other. Without question, the Internet and resulting explosion in information technology have introduced incredible convenience, prosperity, and freedom of expression to nations across the globe.

At the same time, this new technology introduced the world to a new challenge – cybersecurity. Every day, the public is flooded with reports of new breaches, vulnerabilities, or potential risks stemming from weaknesses in the digital infrastructure that drives the 21st century economy. With every new incident, whether it is the theft of consumer data, a nation-state sponsored attack on a corporation, or an intrusion into our nation's critical infrastructure, there is renewed discussion about the need for cybersecurity "solutions." There is relatively little discussion, however, about what this means for businesses and society. For example, how will improved information security affect the pace of innovation? To what extent are consumers willing to sacrifice convenience in the interest of security? How can costly security solutions keep pace with threats that constantly evolve?

Cyber threats are rooted in the fundamental structure of the internet. The same technological and cultural factors that facilitate the strengths of the Internet (e.g., real-time global interaction, rapid innovation, and freedom of expression) enable malicious actors to thrive and create risk in cyberspace. There is no way to "solve" the cybersecurity problem without compromising the benefits of a connected, digital world. Therefore, efforts to minimize the cybersecurity threat require careful consideration of the social, economic, and cultural costs of improved security.

IV. BACKGROUND

A. History and Evolution of the Internet

In the late 1960's, the Advanced Research Projects Agency (ARPA)[1] funded an innovative project called ARPANET. The project sought to realize a concept first described by Massachusetts Institute of Technology researcher, J.C.R. Licklider in 1962 – an interconnected network of computers that could remotely share data and information.[2] In late 1969, four computers located at the University of California at Los Angeles, Stanford University in Palo Alto, the University of California at Santa Barbara, and the University of Utah connected to the ARPANET, proving Dr. Licklider's networking concept and laying the foundation of what is now known as the Internet.[3,4]

What began as a handful of closed networks used by a small and trusted number of parties has evolved into a vast network of networks. These networks range in scale from point-to-point links such as smartphones to massive "backbone" networks that collect, carry, and share information from numerous small networks over vast distances.[5] All of these individual networks

[1] The Advanced Research Projects Agency has since changed their name to the Defense Advanced Research Projects Agency (DARPA). *See* www.darpa.mil.

[2] Internet Society, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (last visited Feb. 26, 2015).

[3] *Id.*

[4] The term Internet was formally agreed upon in 1995 by the Federal Networking Council.

[5] COMMITTEE ON DEVELOPING A CYBERSECURITY PRIMER: LEVERAGING TWO DECADES OF NATIONAL ACADEMIES WORK, NATIONAL ACADEMY OF SCIENCES, AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY: SOME BASIC

are able to interact seamlessly because the Internet was designed be an open platform, based on common architecture and protocols, to transmit data from one location to another. The devices, services, and applications attached to the network remain responsible for processing the data.[6] In other words, the Internet acts simply as a conduit for information.

This open architecture concept is the fundamental basis of the Internet's success. Because the Internet simply transports data and does not discriminate against the applications and devices connected to the network, it creates endless possibilities for innovation. This open framework enabled and continues to foster the development of programs such as email, smartphone applications, and cloud computing. It has introduced previously unimaginable efficiencies for businesses and opened new markets across the globe. It has given individuals a voice and revolutionized the way in which societies learn and consume information. As a result, the Internet has grown to be not just a technological curiosity, but an integral element of modern society.

All of these benefits rely on information technology, comprised of the computing and communications devices and protocols that connect to the Internet.[7] The Internet has therefore driven the massive development and integration of these technologies in our daily lives. Today, we depend on information technology for everything from personal communication to energy distribution. This integration of the Internet and information technologies into nearly every aspect of modern life has created the virtual world commonly known as *cyberspace*.[8] While not easily defined, cyberspace encompasses all networks and information technology, their information and interconnections, both on and off the Internet.[9] While the growth of the Internet and cyberspace provide tremendous benefits to society, they also introduce a new challenge – cybersecurity.

B. Cybersecurity: Threats and Challenges

Complex Systems Create Vulnerabilities

To a standard user of the Internet, the act of visiting a web page is a series of straightforward steps. That user knows to open a browser, enter the web address of the site that he or she wish to view, and then wait for the requested web page to appear. Rarely does one realize, however, the many steps and technological innovations that allow that "straightforward" process to occur. Figure 1 depicts a flowchart of the steps that the information technologies involved in a website request must take in order to successfully display a web page.

CONCEPTS AND ISSUES 21 (David Clark et al. eds., 2014), *available at* http://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic [hereinafter *Primer*].

[6] Internet Society, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (last visited Feb. 26, 2015)

[7] *Primer, supra* note 5, at 8

[8] Lance Strate, *The varieties of cyberspace: Problems in definition and delimitation*, 63 Western J. of Communication 3, 382–83 (1999).

[9] *Primer, supra* note 5, at 8-9

Figure 1 - Flowchart of a Website Request

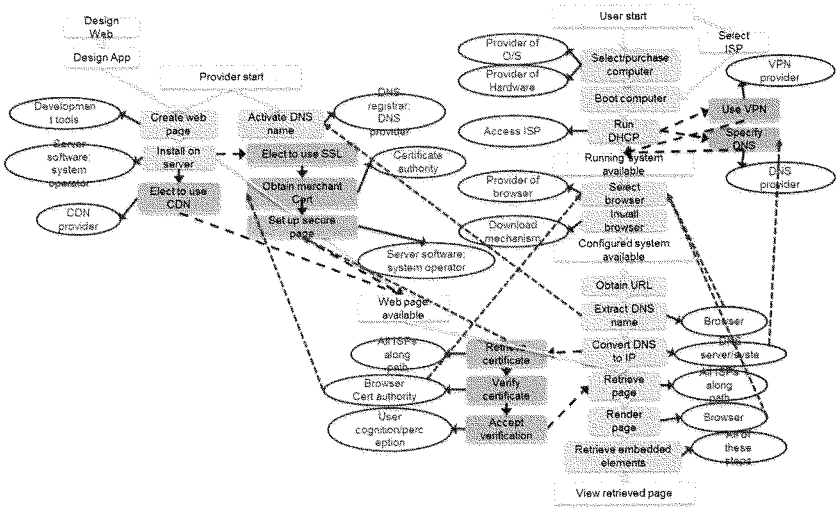


Figure 1 from *Primer, supra* note 5, at 39.

In all, this chart describes dozens of individual steps that must be satisfied by such diverse pieces of technology as the user's browser, the Internet Service Provider's infrastructure, the server hosting the site, and many others, before a website can be displayed. In other words, if any of these numerous steps fail, the user who requested the website will receive an error message instead of the desired content. Misconfigurations, coding errors, and unforeseen issues with the technology itself also may result in a failure. In addition, malicious actors may use each of these steps as a potential attack vector in order to carry out a cyberattack.

While Figure 1 is specific to the act of requesting a web page, this level of complexity exists in every piece of information technology and in every communication facilitated by the Internet. This is due to the fact that the Internet is a massively complex, highly distributed system of systems. At a fundamental level, the Internet is a not a singular "whole," but a web of individual pieces of information technology that are connected by communication protocols. Every device that connects to this web – smartphones, servers, Internet-enabled refrigerators, etc. – is itself a highly complex system of interacting information technology components. In such a system with complex communication protocols, there is a high probability that there are weaknesses that can be used to compromise the reliability or security of that system. When billions of devices are connected together into a distributed network, as they are in the Internet, that probability scales exponentially.

The Fundamental Nature of the Internet Creates an Asymmetric Threat

The fact that the Internet is an open system with many interconnections makes it especially vulnerable to disruption. Furthermore, this vulnerability is asymmetrical: the individual intending to compromise a system can do so at little cost and with little risk of being caught, while the costs of defense, as well as potential consequences, can be large. In other words, a malicious actor need only be in possession of a working Internet connection and an exploitable vulnerability in a target information system in order to compromise it. In addition, the global scale and complexity of cyberspace provide malicious actors the flexibility and relative anonymity to identify or craft an attack that fulfills their objective with minimal fear of consequence. There is also little to no cost for failure. They simply try again and again. Attribution of cyberattacks remains incredibly difficult, and even in cases where cyber "criminals" are indicted, the legal framework prosecuting such cybercrimes remains ill-defined, immature, and bound by geographical borders that do not exist in cyberspace.

Conversely, those responsible for defending information systems must simultaneously keep pace with a wide variety of threats and guard against all possible weaknesses to avoid a breach. This is difficult from a pragmatic perspective – consider Figure 1 and the dozens of steps it takes to view a website, each of which may be vulnerable to attack. In addition, given the low cost, the low risk of consequence, the range of actors and motivations, and the ever expanding scope of vulnerabilities, cyber threats evolve at a rapid pace. This makes it increasingly difficult to identify and eliminate vulnerabilities or malicious actors. A number of recent reports illustrate this challenge:

- Cloud security company Panda Security recorded 15 million new malware samples in the second quarter of 2014, an average of 160,000 new samples every day;[10]

- The PricewaterhouseCoopers (PWC) *Global State of Information Security Survey (GSISS) 2015* report stated that the total number of security incidents detected by survey respondents increased 48 percent from 2013 to 42.8 million, or 117,339 incoming attacks a day;[11]

- Mandiant's *M-Trends 2015* report revealed that approximately 70 percent of victims learned of their breach from an outside source, such as law enforcement. In addition, the report observed that, in 2014, the median number of days that a malicious actor persisted on a system prior to discovery was 205 days.[12]

These challenges are compounded by the numerous avenues for entry available to attackers. For example, malicious actors develop credible looking emails containing a link infected with malware. If an employee inside an organization clicks that link, the attacker has

[10] PANDA LABS, Q2 REPORT 2014, *available at* http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Informe-Trimestral-Q2-2014-EN.pdf.

[11] PWC, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD: KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2015, *available at* http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml. [Hereinafter, *PWC*]

[12] MANDIANT, A FIREEYE COMPANY, M-TRENDS 2015 THREAT REPORT, *available at* https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html.

gained entry. Attackers also can take advantage of weaknesses in the supply chain. They can gain entry to a larger organization by targeting a vendor with weaker security, especially small and medium sized companies, which typically have fewer resources to devote to security.[13]

The issue of cost is not limited to small and medium-sized companies. Cybersecurity is incredibly expensive. According to PWC's survey, organizations budgeted an average of $4.1 million for 2014 for information security.[14] In that same year, cybercrime cost organizations on average $7.6 million globally, and $12.7 million in the U.S.[15] The true costs of cybercrime are difficult to pinpoint given the complexities of calculating the value of lost intellectual property, reputational damage, delays to innovation, etc.[16] In addition, some estimates suggest that more than 70 percent of breaches go undetected.[17]

The complexity of the Internet and cyberspace, the weaknesses that are inherent in that complexity, and the asymmetric cost-benefit between malicious actors and defenders together will make it difficult, if not impossible, to spend, train, or "solve" our way out of cybersecurity problems. The technologies are too complicated, too dynamic, and too diverse. Reliability and security weaknesses exist as part of the Internet ecosystem, and the pace of innovation and adoption of new technologies ensures that new weaknesses will continue to be created and introduced. As our dependence on these technologies increases and they become entwined in everything we do, cyberspace provides limitless and adaptive attack surface.

Balancing Security Needs with Innovation, Convenience, and Usability

Cybersecurity has become a cost-benefit analysis. Governments, businesses, and individuals that depend on the Internet must make security decisions based on their own security, economic, and personal preferences. Improved security means higher costs, longer development timelines, and reduced convenience to consumers. In the current fast-paced, competitive information technology market, each of these factors undermines the economic prospects of a product, service, or business. Further, given the nature of the Internet, the complexity of information technology, and the existence of malicious actors in cyberspace, there is no assurance that a security improvement will be effective. At the same time, failure to provide adequate security can result in grave economic consequences, including but not limited to financial penalties, loss of intellectual property, and lost consumer confidence.

In light of recent, large-scale cyber-attacks, there is renewed interest in developing "solutions" to the cyber threat. While there are opportunities to improve the nation's ability to detect, defend, respond to, and recover from cyber-attacks, it is important not to undermine the benefits of cyberspace. In evaluating potential security measures, government, businesses, and

[13] *PWC*, *supra* note 11, at 8.
[14] *PWC*, *supra* note 11, at 20.
[15] PONEMON INSTITUTE, 2014 GLOBAL REPORT ON THE COST OF CYBER CRIME, *available at* http://h20195.www2.hp.com/v2/getpdf.aspx/4AA5-5207ENW.pdf?ver=1.0.
[16] *PWC*, *supra* note 11, at 11.
[17] *PWC*, *supra* note 11, at 8.

individuals must consider the costs relative to the benefits and the impact on expectations for cost, convenience, privacy, and civil liberties.

C. Looking Ahead

Our daily routines rely on information technologies connected to and dependent upon the Internet and cyberspace. Today, a handheld mobile device can start our cars, unlock our homes, make credit card payments, and monitor our health. A refrigerator can tell us when we are low on milk. We can access Twitter from our outdoor grills. These Internet-enabled devices collectively are referred to as the "Internet of Things," and hardware networking company Cisco believes that they will become so prevalent that by 2020, the number of devices connected to the Internet will exceed 50 billion.[18]

A report by the Institute of Electrical and Electronics Engineers Computer Society (IEEE CS) entitled *IEEE CS 2022* takes that prediction one step farther. The report first states, "[a]s a result of [the] pervasive penetration of computing and communications capabilities, human knowledge, intelligence, and connectivity are increasingly enhanced and augmented by information technology."[19] The IEEE CS then predicts a society that is so embedded with Internet-enabled devices that society's interactions with information technology and the Internet will become so automatic and transparent in daily life that it will create a world of "seamless intelligence."[20] The executive chairman of Google recently provided a similar assessment – eventually, the Internet will become so closely entwined with our daily lives that, to our perception, it "will disappear."[21]

Modern society has become so integrated with information technology and the Internet that cyberspace is no longer simply a place we visit, but a place we live. Through our social media profiles, our bank accounts, our digital health records, and even our browsing histories, we create virtual identities and entrust those identities to cyberspace. Therefore, it is important to examine the benefits and risks of increased integration with information technology, the Internet, and cyberspace.

V. ISSUES

The following issues may be examined at the hearing:

- How the challenge of cybersecurity is inexorably connected to the history and structure of the internet;
- The economic, social, and cultural factors that contribute to the challenge of cybersecurity;

[18] Dave Evans, Cisco, The Internet of Things: How the Next Evolution of the Internet is Changing Everything (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[19] Hasan Alkhatib et al., IEEE Computer Society, 2022 Report (2014), *available at* http://www.computer.org/cms/Computer.org/ComputingNow/2022Report.pdf.

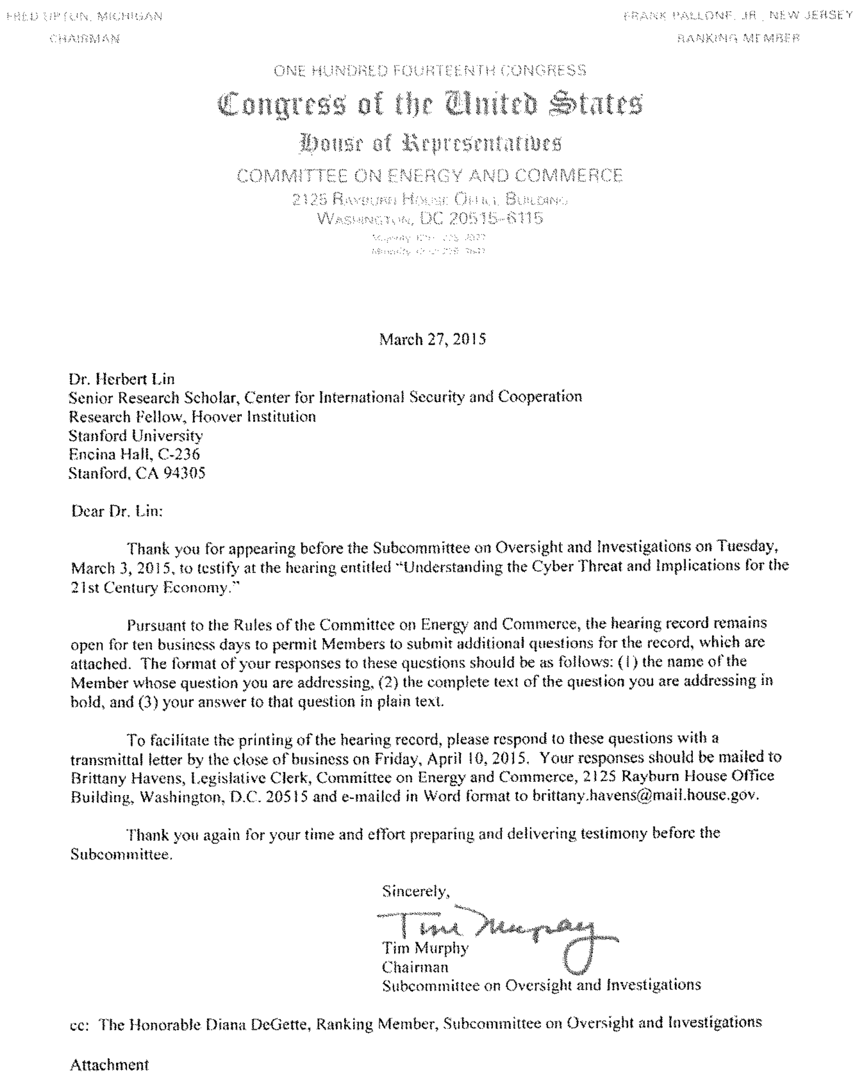
[20] *Id.*

[21] Georg Szalai, *Google Chairman Eric Schmidt: "The Internet Will Disappear,"* The Hollywood Reporter, Jan. 22, 2015, *available at* http://www.hollywoodreporter.com/news/google-chairman-cric-schmidt-internet-765989.

- The tradeoffs associated with effective security;
- Why there is no immediate solution to the cyber threat;
- The importance of cybersecurity to commerce and the economy in the 21st century;
- Current trends and emerging threats; and,
- Expected advancements in technology and their relationship to cybersecurity.

VI. STAFF CONTACTS

If you have any questions regarding this hearing, please contact John Ohly or Jessica Wilkerson with the Committee staff at (202) 225-2927.



FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

March 27, 2015

Dr. Herbert Lin
Senior Research Scholar, Center for International Security and Cooperation
Research Fellow, Hoover Institution
Stanford University
Encina Hall, C-236
Stanford, CA 94305

Dear Dr. Lin:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, March 3, 2015, to testify at the hearing entitled "Understanding the Cyber Threat and Implications for the 21st Century Economy."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, April 10, 2015. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to brittany.havens@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Attachment 1—Additional Questions for the Record

The Honorable Tim Murphy

1. Each witness provided a slightly different perspective on cyber threats and the challenge of cybersecurity, extending from the past, to the present and future.

    a. Are there areas where you feel there is a common view or shared theme and what is it?

I'm quite confident that we all share the view that cybersecurity is an issue of true national importance, that we are not doing as well as we could against the cyber threats we face, and that the road ahead to improving the nation's cybersecurity posture significantly will be rocky and difficult.

    b. If there was one fundamental message you want Congress and the public to understand about cybersecurity, what would it be?

There are tradeoffs to be made for better cybersecurity, and if you want better cybersecurity for the nation, you had better be willing to make tradeoffs against other things that you hold dear. As an example that I emphasized in my testimony, market forces virtually require that reducing time-to-market for innovative products and services takes precedence over building these products and services with good security from the start.

    c. Are there specific issues or areas of this issue that do not receive an appropriate level of attention?

The fact that there are tradeoffs between cybersecurity and other desirable attributes or public policy outcomes is not discussed or appreciated adequately. For example, in recent months, the FBI has asserted the need to have access to encrypted information in pursuit of their mission, while much of the information technology industry has argued that building in the capabilities for providing such access to law enforcement authorities would reduce the security of their products and services in ways that are detrimental to their marketplace acceptance. Both side are being truthful, and there is no way to fully reconcile the two conflicting positions. The nation must make a tradeoff between two good things—and the need to make that tradeoff has been obscured by absolutist rhetoric on each side asserting that the other side has no facts or argument to support it.

2. As the promise of innovation connects more of our lives to cyberspace — from smart pacifiers to cars that communicate with each other — cyberspace becomes, in theory, a limitless attack surface.

    a. How do we manage the risks presented by "smart devices" and the Internet of Things while also enjoying the benefits and convenience they offer to society?

The security problems posed by smart devices and the Internet of Things are not different in principle than those posed by other computational devices. However, smart devices and the IOT pose a problem of scale—along with hundreds of millions or even billions of new Internet users coming online in the next decade or so, smart devices and the IOT have the potential to make the security problem much, much worse. In addition, widespread adoption of IOT devices suggests that they will be relatively inexpensive, which gives vendors less ability to build in cybersecurity capabilities. And they may well be installed in place where they are not regularly updated, which means that security patches are less likely to be installed frequently. Finally, the public attention given to cybersecurity for smart devices and the IOT by vendors and advocates is certainly greater today than it was in the past for other computing devices, but whether security *practices* have actually changed significantly is an open question.

Managing cybersecurity risks is largely a matter of persuading or incentivizing vendors and users to pay more attention to cybersecurity issues, and I prefer the use of market forces to do that over direct regulation. Harnessing market forces to this end means that something must happen that adjusts the market forces in that direction; leaving it all to the vendors and users to decide on their own what they want to do regarding cybersecurity is a recipe for inaction on the security front. But there is no consensus on the steps that might be needed to adjust market forces. For example, some people believe that liability of cybersecurity defects would help to push vendors to pay more attention to cybersecurity; others believe that liability would dampen innovation significantly. For every measure proposed to harness market forces, good reasons can be assembled to oppose it.

b. As more devices connect to cyberspace and interact with one another, what challenges does this present for how security professionals or companies anticipate potential vulnerabilities or risks?

More connected devices mean a more complex environment to analyze for security risks. Today's analytical tools are inadequate for this task. Security companies and professionals will have even greater difficulty in undertaking such analysis in the absence of better tools.

c. How do we assess the security of individual products relative to the security of the system as a whole?

Today's systems are composed of a variety of components. Even when those components are individually known for sure to be trustworthy, there is no guarantee that the system as a whole is itself trustworthy. And the trustworthiness of individual components is difficult to assure as well.

d. In such an interconnected world, how do you draw the line between a potential vulnerability and a realistic vulnerability? In other words, just because something is possible, how important is it to assess the probability that it will occur?

It is important to distinguish between two different types of threat. One type (call it Type A) is a threat that does not change in reaction to a change in the target's defenses. Typically, the perpetrator of a Type A threat does not care very much about success against a particular individual target, but rather relies on statistical likelihood to succeed. The canonical example is a criminal trying to steal credit card numbers—he does not particularly care whose credit card numbers he obtains, only that he obtains as many as he can get. A second type (call it Type B) is a threat that does change in reaction to a target's defenses. The perpetrator of a Type B threat cares very much about success against a particular target—for example, the CEO of a major defense firm. When that CEO's security people deploy defenses to thwart a particular kind of attack, the Type B threat will morph into something else and the perpetrator will try again. And the perpetrator will try repeatedly until successful.

The difference between Type A and Type B threats is that against a Type B threat, one must address essentially all vulnerabilities, independent of likelihood of exploitation. Why? Because the Type B threat can take advantage of any vulnerability. By contrast, when facing a Type A threat, probability does matter because by definition, the Type A threat can only take advantage of a given set of vulnerabilities and will not change. Thus, addressing the vulnerabilities most likely to be exploited by a Type A threat has significant value in the sense that such action will extend the period of time in which a Type A threat will be unsuccessful.

3. Quite a few respected technologists — at Google, and also at the Institute of Electrical and Electronics Engineers Computing Society — have theorized that in the future, the Internet will be so integrated into our daily lives that it will become "invisible" and provide "seamless intelligence."

    a. Can you expand a little more on how exactly a world with an "invisible" Internet would work?

Today's electrical power system provides an analogy. There are a huge number of devices in our homes and office and factories that use electricity. But for the most part, the electrical infrastructure is invisible to us—except when it fails. The vision offered by Google and the IEEE CS is an appealing one of information at the automatic beck and call of any device whose operation can be improved or is enabled through the use of the appropriate information. And the Internet is expected to be the platform through which such information is delivered at the appropriate times.

    b. Do you agree with these predictions? Why or why not?

I agree with them in the sense that I don't believe that the vision is fundamentally impossible to achieve, and that the world depicted could be a desirable one—provided that other concerns are adequately addressed, such as security, resilience, and privacy. But whether these other concerns will in fact be adequately addressed is anyone's guess. Standing in the way of achieving this vision, entirely apart from the very formidable technical challenges, is the need for a societal consensus about the right balance between many desirable qualities of this world. And at this stage, I don't see what that consensus might be or how it might emerge.

4. No matter how much money a company invests in security software, training and other cybersecurity measures, they still remain vulnerable to the insider threat. This can range from the intentional actor — such as a disgruntled employee stealing information or letting the bad guys in — to inadvertent actors — such as an employee clicking an infected link in a targeted phishing email.

    a. Will companies ever be able to prevent internal threats — employees lowering the proverbial draw bridge — regardless of whether their actions are intentional or unintentional?

No. They may be able to detect such individuals after they have done their dirty work, but if the individual(s) in question is or are willing to bear the consequences of being caught, there is no way to thwart entirely the insider threat. Note also that a goal of many outsider threats is to achieve insider status, a goal often reached through social engineering against an insider.

b. if it can never be eliminated, does it come down to managing risk? Are there proven strategies to minimize this risk?

Yes, it is a matter of risk management. And some strategies for minimizing risk are better than others. But the optimal strategy for any given organization is highly dependent on the nature of that organization; one size does not fit all in the world of risk management. In other industries, risk management techniques have evolved to address the insider threat. For example, in the financial industry, techniques such as double-entry accounting, separation of duties, and periodic audits have emerged as useful risk management techniques. All of these techniques involve some degree of business process redesign, which is inevitably one of the

c. How significant of a challenge is this to those evaluating the cost benefit of security measures?

It's a huge challenge. For example, those trying to do cost-benefit analysis of security measures need a lot of data to make their assessments. That means they need to collect it, and identify specific ways in which security measures can fail. Sometimes such data is available; more often, it is not. Even when it is, analysts need to know how to use it. As a rule, it is easier to quantify what a security measure costs, although one must be careful to account for non-obvious costs such as loss of convenience, availability, and so on. But it's much harder to quantify how many of those bad things were prevented from happening because of the security measures or for some other reason.

5. Information sharing, though it has its benefits, is still a reactionary solution. Someone has to first suffer an attack before that threat information can be shared, and oftentimes the attackers change their signatures from target to target.

a. How does information sharing help reduce the gap between cybersecurity capabilities and threats to cybersecurity described in your written testimony?

Information sharing can help in a number of ways. For example, knowledge that you have been attacked may alert me to the possibility that I have been attacked, or am about to be attacked. The former case may prompt me to do an investigation to determine if in fact I have been attacked, an investigation that I would not otherwise do. The latter case may prompt me to take additional defensive measures, above and beyond those that I would have taken in the absence of such information. At a technical level, information sharing may help me to pinpoint the threat that is attacking me.

There is a lot of focus on signatures when it comes to information sharing.

i. Are signature-based defenses effective? Why or why not?

Signature-based defenses are effective against a certain kinds of threat but not against other kinds of threat. An example is that not all signatures of possible threats are known in advance of that threat's strike. A zero-day vulnerability is one whose existence was not known prior to an attacker's use, and thus against which no specific defense could be mounted. Note that signatures are only a subset of information that might be shared.

b. How does information sharing fit into the broad picture of the cybersecurity challenge?

i. Does it offer opportunity beyond improving our defensive capabilities?

If one is willing to include under the rubric of "defensive capabilities" issues such as attack detection and remediation (as would be proper), sharing has value far beyond attack prevention; these include detection; remediation. Moreover, information sharing of all kinds is at the heart of successful collaborations. Sharing threat information may not directly contribute to business collaboration, but it may be the first step towards establishing a trust between two organizations that would enable them to share other kinds of information.

6. Is it possible to quantify the benefits of the Internet and information technology relative to the cost of security?

a. In other words, is it possible to calculate the economic benefits of these technologies relative to the economic costs of cybersecurity, including prevention and response in the event of a breach?

There is a substantial cottage industry devoted to making such calculations, but I'm sorry to say that their estimates differ from each other significantly. Moreover, their methodologies are highly questionable. So from my perspective, I can say that I've never seen a comparison of these costs that I believe or have any faith in.

b. How about the social, cultural or other less tangible benefits?

These benefits are even harder to quantify. As an example – what dollar value would one put on the ability of Americans to communicate freely with each other through electronic means? One could estimate the revenues of the telecommunication industry and use it as a proxy for the monetary value that we as a nation assign to communications. But as a U.S. citizen, I value my First amendment rights even when I am NOT communicating with others—and there's essentially no amount of money that anyone could give me that would compensate for the loss of such rights.

c. Is there value in this?

I interpret the question to mean – is it valuable to quantify the value of the Internet and information technology and the costs of keeping them secure? Yes, I think there is value in the exercise because the exercise forces the analyst to consider various factors systematically, but it will be important to refrain from treating the numbers that emerge from such an analysis as anything more than suggestive. Any particular analysis is likely to omit some very important factors and to have very large uncertainties about the estimates it does make.

7. Discussions about cybersecurity often focus on prevention or keeping actors out of system
   - Is this the right way to approach this issue?
      a, If there is no guarantee the bad guys will not get in, should the emphasis shift to a focus on resilience rather than prevention?

In the long run, both prevention and resilience have meaningful roles to play, but I agree with the thrust of the question that the value of resilience is underappreciated. Today's world is largely one of perimeter defense, a paradigm in which you can cleanly separate "inside" from "outside". The boundary between inside and outside is the perimeter, which is where most defensive efforts are concentrated. But with this model, an attacker that is successful in penetrating the perimeter then has free rein inside the system, with little to impede his efforts. Consider, for example, that in any organization, the information technology on which it relies is the end point in a long supply chain, and compromises to supply chain security enable the attacked to be present "inside" even before the perimeter of the system is established. Savvy organizations are learning to operate in a compromised information technology environment, with all that such operation implies, though perimeter defenses are still valuable in reducing the scale of the problems they face inside the perimeter.

I also note that even defining a perimeter is often problematic in a world in which the components that make up the system originate in myriad places over which the system owner or operator has no control. Even an individual hardware chip may have circuitry inside that comes from many different and possibly untrustworthy sources.

b. Why is the concept of resilience important to effective cybersecurity?

Consider the value of file backups. You back up your files so that if a file is accidentally deleted, you can retrieve a recent copy and not lose most or all of the work that went into creating it. It's not a big step to imagine a bad guy deleting your precious file deliberately, but even in this case, the backup has significant value. In this context, backup is a part of effective resilience-based cybersecurity.

Backups are not free, however. You need to expend some time and effort to perform a backup. So you work somewhat less efficiently because you don't entirely trust your environment—that is, you operate under the assumption that environment may be (probably is) compromised.

The same general lessons apply to any other aspect of resilience. You pay something in time and effort to preserve some essential functionality—you hedge against disaster.

c. How does resilience support a risk-based approach to cybersecurity?

You select specific features of a resilience architecture depending on what you care about most. For example, a bank might care much more about preserving the integrity of its data than its confidentiality—that is, it would be much worse for a bank to have its records scrambled so it did not know what was in the accounts of every depositor than for those records to be revealed to the outside world. Neither is good for the bank, of course, but under these circumstances, the bank might well provide extra support for resilience efforts to enhance data integrity than data confidentiality.

8. Dr. Lin, in your testimony you said that "complexity is the enemy of cybersecurity."

    a. Is it possible to reduce this complexity?

        i. If yes, what are the consequences?

        ii. If no, why not?

It is unquestionably true that some reductions of complexity are possible through more careful design given a set of performance requirements for a system. But in my judgment, by far the biggest driver of complexity is that we want our systems to do more and more. That is, our appetite for greater functionality in our systems is essentially unlimited. Any serious attempt to reduce the complexity of systems has to start out by someone being willing to say "no" to demands for more functionality.

Based on what you said about the complexity of a system increasing when additional components are connected to it, the "Internet of Things" is going to exponentially increase the complexity of the Internet.

    b. What does this mean for the governments, businesses, and individuals that are going to use these connected devices?

I don't disagree with the implication that the IOT will make the internet much more complex, and thus more insecure. We can mitigate it to some extent, but for many people, the benefits of the IOT are not so compelling that it is worth the added insecurity that will result. I personally expect to be a late adopter of these technologies for exactly this reason.

    c. How will this influence or reshape current cybersecurity practices?

I suspect the most important influences will be that it will increase the demand for people knowledgeable about cyber security

9. In the last few years, there have been several significant compromises and vulnerabilities discovered in regards to digital certificates and Certificate Authorities, two of the best well-known being the compromise of DigiNotar and the recent LenovoiSupertish revelations. This raises questions as to whether the digital certificate model is providing an adequate level of security for users of the Internet.

    a. What are the weaknesses in the digital certificate model?

i. How significant are these weaknesses?

ii. Can these weaknesses be eliminated or adequately mitigated?

Certificate authorities exist to "certify" that two parties actually in remote electronic contact with one another in fact correspond to the parties' expectations. John thinks he is talking electronically to George; a certificate authority certifies that John is really talking to George and not to Sam. In the absence of a reliable certificate authority, John might in fact be talking to anyone. A digital certificate is an electronic credential issued (in this case) to George that certifies that anyone relying on the certificate and communicating with George is indeed talking to George.

Therefore, a certificate authority must be trustworthy. Its technical protections must be robust enough to withstand attacks intended to compromise its certifications. Its management protections must be robust enough that it does not issue certificates improperly (e.g., does not issue a certificate saying "George" to Sam.) But over the years, the number of certificate of authorities has grown. With such growth the variance in the trustworthiness of the best and the worst has grown, and it is of course the least trustworthy certificate authorities that are the most vulnerable targets for compromise. For these untrustworthy certificate authorities, sloppy implementation of technologies and processes for issuing and managing certificates is common.

b. Are Certificate Authorities subject to any form of oversight?

i. If so, by whom and how does this function?

ii. If not, would enhanced oversight help address the weaknesses examined in Question I ? Why or why not?

To the best of my knowledge, certificate authorities are not subject to government oversight as a general rule. Sometimes a government agency itself will serve as a certificate authority, and in such cases, it is by definition subject to government control, but that is not necessarily the same as being obliged to conform to a variety of standards.

I have not thought through the pros and cons of government oversight of certificate authorities. One immediate problem is that certificate authorities are international in reach (that is, internet users all over the world may come rely on a particular certificate authority) and yet the CA itself is subject to the jurisdiction of only one country. It would be easy, in principle, to set up CAs in places with weak or no oversight—an analogy is the maritime flag of convenience that allows ship owners to evade regulation associated with states more concerned about maritime safety. Users could choose to not use CAs that are not subject to adequate oversight, but as a rule that would require users to take specific action to do so—and many users would fail to take such action, and wind up trusting untrustworthy CAs.

c. Are there alternatives to the digital certificate model?

i. If so, what are they?

ii. If not, how can the current digital certificate ecosystem be improved?

There are a variety of mechanisms that could replace certificate authorities, but all of them have drawbacks as well as advantages. The fundamental problem is that the need for a trust mechanism cannot be avoided, and where trust is involved, trust can be betrayed. One can increase the difficulty of betrayal, but only at the cost of less convenience.

To the best of my knowledge, an authoritative study on the strengths and weaknesses of the CA model and alternatives to it has not been performed; such a study could be performed well by the National Academies. (Full disclosure – I worked for the National Academies for many years, am in a state of semi-retirement from the Academies, and still consult for them from time to time.)

10. In your written testimony you describe how tradeoffs between security, innovation, and convenience are unavoidable.

a. What is required to achieve consensus on tradeoffs? Is such a consensus possible?

Tradeoff are hard for people to make. By definition, a tradeoff involves having more of X and having less of Y, when both X and Y are good things to have. The problem arises when you value X more and I value Y more. Making tradeoffs thus involves compromise, in which neither you nor I get as much of X and Y as we could have, and unfortunately we see today that compromise in the policy arena is often regarded as a problem rather than as an approach to a solution.

b. Is there a way to narrow these tradeoffs, such as by developing a technology that is at once secure as well as convenient? How much more difficult is this kind of development?

The question above embeds an important insight—it is indeed often possible to do better on both security and convenience. But it is hard to do—harder to focus on two attributes simultaneously than just focusing on one. This will increase the time needed for development—and will potentially delay the arrival of the new technology that is both convenient and secure. If a competitor puts out a product that is convenient and less secure first, it is likely that the company paying extra attention to security will lose in the marketplace. This does not mean it should not be done – only that it will happen less often than would be desirable.

11, In your testimony, you described a two-part goal for reducing threats in cybersecurity. The first is reducing the gap between average cybersecurity posture and the best possible cybersecurity posture. The second is research and development of the best possible cybersecurity posture,

a. Between these two goals, which is more attainable? Why?

The Part 1 gap requires the application of existing technical knowledge for better security. We may lack the nontechnical knowledge that would drive the further adoption of known security technologies and policies, but at least we know what some of these better technologies and policies are. The Part 2 gap is one where we don't even have the technical knowledge, let alone knowledge about how to drive adoption and use. So I think the Part 1 gap is easier to close.

b. Which is more critical to our long term economic success?

I think they are both critical, but I can't make the relative judgment you are asking me to make.

c. Are we making progress on either goal? If so, how and what is driving this change?

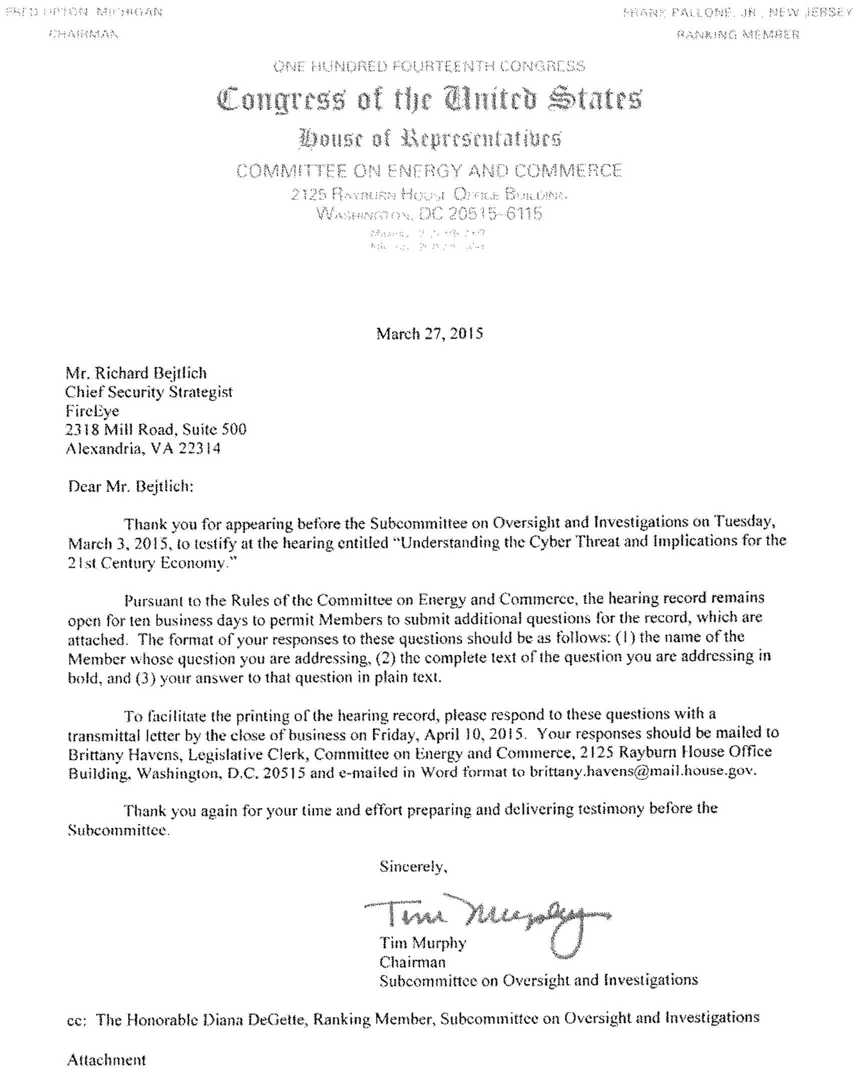
We are making progress in the sense that we are better at cybersecurity than we were a decade ago. For the Part 1 gap, for example, the last 10-15 years have seen the study of the economics of cybersecurity become a respectable field of research. Economics is a key driver of where and how cybersecurity technologies are adopted, and we are gaining some insights into the incentives and disincentives for cybersecurity. But taking action on these economic insights remains a problem, for reasons based on the lack of consensus regarding tradeoffs I mentioned in my testimony. For the Part 2 gap, a variety of technically focused research has resulted in new technologies and approaches to cybersecurity that have some promise. But as I discussed in my testimony, what we ask of our information technology grows at a more rapid rate than our knowledge about how to remediate the accompanying security problems, and so despite these efforts, the gap continues to grow—though not as fast as it would in the absence of these research efforts.

Lastly, keep in mind that the skill and sophistication of the bad guys continues to grow. As I noted in my testimony, they do not simply wait around for the gap to be closed and then go home after it has been closed. They adopt new techniques, find new targets, employ new tactics and technologies for their dirty work—which means that improving cybersecurity is a long-term process rather than a one-time event.

The Honorable Markwavne Mullin

1. It seems like whenever we start talking about the challenges that come with responding to any emerging industry or emerging threat, the issue of workforce development is front and center. With something like the engineering industry, we know we need to engage more students in STEM education, should we be treating the IT industry in the same way?

There isn't an IT corporate executive around who believes that the talent pool for IT workers is sufficiently deep and broad. The basic problem is that the skills and added value that different IT workers bring to the table differ enormously—and innovation in IT is driven by the best of the best, rather than by many workers of average talent working together. If this is true, there is a high premium on creating environments in which the best of the best can be identified and nurtured and persuaded to work in the IT industry.



FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congreſs of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 Rayburn House Office Building
Washington, DC 20515-6115
[illegible]
[illegible]

March 27, 2015

Mr. Richard Bejtlich
Chief Security Strategist
FireEye
2318 Mill Road, Suite 500
Alexandria, VA 22314

Dear Mr. Bejtlich:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, March 3, 2015, to testify at the hearing entitled "Understanding the Cyber Threat and Implications for the 21st Century Economy."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, April 10, 2015. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to brittany.havens@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Response to Questions

from the

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

by

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

13 April 2015

Thank you for the opportunity to answer questions for the record, prompted by the hearing "Understanding the Cyber Threat and Implications for the 21st Century Economy," 3 March 2015. I have answered those that fall within my area of expertise, to the best of my ability.

The Honorable Tim Murphy

1. **Each witness provided a slightly different perspective on cyber threats and the challenge of cybersecurity, extending from the past, to the present and future.**

   a. **Are there areas where you feel there is a common view or shared theme and what is it?**

"Cyber security" is as expansive a topic as "health" or "crime" or "war." No one achieves a level of excellence, or approaches some degree of understanding, without concentrating on one or two specialties. One can approach the topic from different levels, such as technology, tactics, operations, strategy, and policy. There are few, if any, shared definitions, measurements of success, or even terminology. There is no digital security equivalent to the "Generally Accepted Accounting Principles" (GAAP) of the financial world.

Given this background, it is difficult to find shared themes. However, many security professionals would agree that, in the digital world, offensive actors have an inherent advantage over defensive actors.

   b. **If there was one fundamental message you want Congress and the public to understand about cybersecurity, what would it be?**

Constituents should expect organizations to be compromised by malicious actors. However, it is the speed and quality of the incident detection and response process that determines if the intrusion results in serious damage to the organization or the information it holds. Defenders win when they stop intruders from accomplishing their mission, not necessarily because defenders keep every invader from gaining unauthorized access.

All organizations should prioritize identifying and removing intruders from their networks. Only after an organization makes incident detection and response the primary security focus should they allocate resources to preventive measures, such as by mitigating software vulnerabilities and misconfigurations. Intruders are already infiltrating targets. It does no good to build higher walls when an invader is already on the inside.

Unfortunately, it is impossible for all organizations to defend themselves using this strategy. Every organization connected to the Internet cannot individually defend itself from mid- to high-level threat actors, such as organized criminal groups and nation-state hacking units. Only the best-resourced, best-led, and best-postured organizations can successfully implement a strategy that frustrates adversary operations.

This situation is not unique to the digital world. One finds the same situation in the physical world. Therefore, we must apply the same range of defensive measures found in the physical world, and abandon the notion that technical measures alone will "solve" the problem. I agree with the message in Bruce Schneier's book Liars and Outliers. He asserts that technical solutions, or "security systems," constitute about 10% of risk mitigation in the physical world. The remaining 90% is a result of "societal pressures," namely moral, reputational, and institutional forces. We must apply more of these other forces to digital security, and stop expecting technical systems to implement most of the security we need in cyber space.

c. **Are there specific issues or areas of this issue that do not receive an appropriate level of attention?**

Congress should support research for a United States Cyber Corps, or Cyber Guard. Possible roles for this organization include helping domestic and foreign allied organizations defend themselves in cyberspace. Research would determine if this group is needed, and how it would be organized, trained, and equipped.

Congress should also support research for a United States Cyber Force. This unit would be the next step for the existing Cyber Command. Research would determine if this group is needed, and how it would be organized, trained, and equipped.

2. **As the promise of innovation connects more of our lives to cyberspace – from smart pacifiers to cars that communicate with each other – cyberspace becomes, in theory, a limitless attack surface.**

a. **How do we manage the risks presented by "smart devices" and the Internet of Things while also enjoying the benefits and convenience they offer to society?**

As a starting point, all vendors should adopt secure software development lifecycles, and other practices, from the Building Security In Maturity Model (www.bsimm.com). Organizations processing information should adopt the Critical Security Controls (www.counciloncybersecurity.org/critical-controls) and consider cyber insurance to better manage risk.

b. As more devices connect to cyberspace and interact with one another, what challenges does this present for how security professionals or companies anticipate potential vulnerabilities or risks?

Digital security is not strictly a technical problem. Many elements of society can play a role. We need to write histories of security incidents to provide examples for students, practitioners, and policy makers. We need courses and seminars that teach business and agency executives how to lead organizations under constant digital attack. We need to support the development of research-driven and field-tested strategies to defend information and users.

c. How do we assess the security of individual products relative to the security of the system as a whole?

Assuming the developers build software following principles such as BSIMM, the next step should be inviting security researchers to test software using bug bounties and similar exercises. Once deployed in the field, owners must monitor interactions with the software. Vendors must provide responsive support mechanisms to accept and act on security problems discovered in real-life conditions.

d. In such an interconnected world, how do you draw the line between a potential vulnerability and a realistic vulnerability? In other words, just because something is possible, how important is it to assess the probability that it will occur?

History has shown that, over time, someone will identify and eventually exploit vulnerabilities in all software. The more popular the product, the more scrutiny it will receive.

Therefore, developers and owners must prioritize the attention they give to the most critical systems and data. It is more important to develop and defend a system that operates industrial control systems, or that processes financial or sensitive personal data, than it is to develop and defend an Internet-connected toy. While it may be possible to exploit an Internet-connected toy to gain access to more important resources, defenders must prioritize their time and effort.

3. Quite a few respected technologists – at Google, and also at the Institute of Electrical and Electronics Engineers Computing Society – have theorized that in the future, the Internet will be so integrated into our daily lives that it will become "invisible" and provide "seamless intelligence."

a. Can you expand a little more on how exactly a world with an "invisible" Internet would work?

No comment. Please ask the original source.

b. Do you agree with these predictions? Why or why not?

No comment.

4. No matter how much money a company invests in security software, training and other cybersecurity measures, they still remain vulnerable to the insider threat. This can range from

the intentional actor – such as a disgruntled employee stealing information or letting the bad guys in – to inadvertent actors – such as an employee clicking an infected link in a targeted phishing email.

a. **Will companies ever be able to prevent internal threats – employees lowering the proverbial draw bridge – regardless of whether their actions are intentional or unintentional?**

No. If it is possible for an authorized user to access an information resource, it is possible for an unauthorized user to eventually do so as well.

b. **If it can never be eliminated, does it come down to managing risk? Are there proven strategies to minimize this risk?**

I recommend referencing the The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (resources.sei.cmu.edu/library/asset-view.cfm?assetID=30310).

Everyone is familiar with the insight that an intruder only needs to exploit one victim in order to compromise the enterprise.

However, few are familiar with the insight that the defender only needs to detect one of the indicators of the intruder's presence in order to initiate incident response within the enterprise.

I call this situation the "intruder's dilemma" (taosecurity.blogspot.com/2009/05/defenders-dilemma-and-intruders-dilemma.html). Therefore, one defensive strategy is to audit and log user actions, thereby introducing more artifacts that an attacker must avoid creating in order to remain stealthy.

A second strategy is to reduce the amount and value of data collected by an organization, and to compartmentalize access to the data that remains.

c. **How significant of a challenge is this to those evaluating the cost benefit of security measures?**

It is a question of relative risk. The likelihood of an insider event is statistically less than that of an outsider event. However, insiders cause more damage in some cases. Also, once within a network, outsiders often act and appear as insiders.

5. **Information sharing, though it has its benefits, is still a reactionary solution. Someone has to first suffer an attack before that threat information can be shared, and oftentimes the attackers change their signatures from target to target.**

a. **How does information sharing help reduce the gap between cybersecurity capabilities and threats to cybersecurity described in Dr. Lin's testimony?**

Threat intelligence can help defenders more quickly resist, identify, and respond to intrusions, but only if the organization is postured to succeed. Until one invests in sound strategy, processes, people and technology, no amount of information sharing or threat intelligence will be sufficient.

I recommend organizations start their information sharing programs by taking advantage of free offerings. For example, Critical Stack (www.criticalstack.com) provides a marketplace for nearly 60 free intelligence feeds (intel.criticalstack.com). Defenders can integrate these sources before evaluating commercial sources.

b. There is a lot of focus on signatures when it comes to information sharing.

i. Are signature-based defenses effective? Why or why not?

Some aspects of intruder activity can be codified into signatures. When defenders apply these signatures to threat activity, they can identify and perhaps stop some malicious behavior. Intruders, however, learn to bypass many signature-based approaches. In those cases, defenders need to use tactics, techniques, and technologies that do not rely on signatures. For example, so-called detonation chambers can safely execute malicious code, observe subsequent behavior, and derive new ways to detect and stop intrusions.

c. How does information sharing fit into the broad picture of the cybersecurity challenge?

i. Does it offer opportunity beyond improving our defensive capabilities?

Sharing threat intelligence refers to three cases: 1) from the government to the private sector; 2) within the private sector; and 3) from the private sector to the government. All three face challenges.

In the government-to-private scenario, I encourage officials to grant clearances to private security teams not working on government contracts. The government should also augment its narrative style intelligence reports with digital appendices that list threat data in machine-readable form, similar to that offered by the OpenIOC format (www.openioc.org).

In the private-to-private case, I recommend creating information sharing groups. Adversaries often target whole sectors at once, so it helps to have peer companies compare notes.

The private-to-government case is the most contentious, for two reasons.

First, companies are reluctant to publicize security breaches, beyond what is necessary to comply with laws and standards. The private sector fears penalties if they disclose incidents to the government. Companies should not be held liable for voluntarily reporting incidents. Accordingly, the White House proposal prohibits the use of so-called "cyberthreat indicators" in any regulatory enforcement action.

Second, some privacy advocates believe that liability protection will let companies submit customer personal information to the government. This position does not reflect the reality of threat intelligence as defined earlier. Proper threat intelligence contains tactics, tools, and procedures used by intruders to abuse software and networks. It does not contain personal data from or about customers, if properly formatted.

6. Is it possible to quantify the benefits of the Internet and information technology relative to the cost of security?

a. In other words, is it possible to calculate the economic benefits of these technologies relative to the economic costs of cybersecurity, including prevention and response in the event of a breach?

I recommend discussing these issues with companies who write breach insurance policies.

b. How about the social, cultural or other less tangible benefits?

While it may not be possible to quantitatively measure the benefits, it is qualitatively possible. Following recent intrusions, for example, corporate executives have lost their jobs.

c. Is there value in this?

No comment.

7. Discussions about cybersecurity often focus on prevention or keeping actors out of system - Is this the right way to approach this issue?

a. If there is no guarantee the bad guys will not get in, should the emphasis shift to a focus on resilience rather than prevention?

It depends on the definition of "resilience." I fear too many advocates define resilience as "continuing to work despite being compromised." If that is the definition, we already operate "resilient" systems, at least when intruders choose only to steal information, and not modify or destroy it.

Organizations should always seek to prevent as many intrusions as possible, but they should not limit their security program, or defensive mindset, to prevention.

b. Why is the concept of resilience important to effective cybersecurity?

I prefer to define resilience in terms of process and operations. For example, an organization operates a resilient security program when it can detect and remove intruders before they accomplish their mission.

In some cases, resilience means using backup systems that do not rely on the Internet. For example, a soldier in the field should know how to use a map and compass if she loses Global Positioning Satellite contact. A company should have a means to communicate with employees that does not require email and Internet Protocol-based phones.

c. How does resilience support a risk-based approach to cybersecurity?

It depends on the definition of a "risk-based approach." I fear too many advocates define the phrase as "decide what we think is a problem, and try to prevent it." That is a failing strategy. I recommend security leaders start by addressing the problems they are already facing. They should prioritize defenses based on what is happening, not what they fear might be happening. In too many organizations, "risk" is an outdate concept. Because of adversary actions, "risk" has evolved from a "possibility" to a certainty, but executives continue to act in terms of possibility.

d. Based on your experience, are companies adopting a risk-based approach to cybersecurity – whether it is the NIST framework or a similar model?

i. Do you have a rough approximation of how prevalent this is? Is it the dominant approach? Increasing?

Companies are adopting frameworks in order to be compliant with regulations and to withstand third party scrutiny. Most companies talk about applying "risk-based approaches," and they use the flawed definition I described earlier.

ii. Does this vary by industry or size of company?

I have no data on this topic.

1. If so, what are the driving factors?

No comment.

8. In Dr. Lin's written testimony he stated that "complexity is the enemy of cybersecurity."

a. Do you agree with this assessment?

Yes. "Cyber security" is a "wicked problem." (Please see my later answers for an explanation of this term.)

b. Is it possible to reduce this complexity?

i. If yes, what are the consequences?

I can offer one example from the industrial control system world. Complexity can be reduced by replacing, where possible, general purpose hardware and flexibly programmed operating systems and applications with purpose-built hardware and deterministic, limited programs. For example, there are few, if any, technically sound reasons to introduce general purpose hardware and flexibly programmed operating systems and applications into certain industrial control systems. Customers buy these systems because they are cheaper. Unfortunately, they expose a greater surface area due to their complexity, and import vulnerabilities that were previously not present.

ii. If no, why not?

9. In the last few years, there have been several significant compromises and vulnerabilities discovered in regards to digital certificates and Certificate Authorities, two of the best well-known being the compromise of DigiNotar and the recent Lenovo/Superfish revelations. This raises questions as to whether the digital certificate model is providing an adequate level of security for users of the Internet.

a. What are the weaknesses in the digital certificate model?

Moxie Marlinspike (www.thoughtcrime.org/) is the authority on the problems with digital certificates. I recommend asking him to obtain definitive answers.

i. **How significant are these weaknesses?**

No comment.

ii. **Can these weaknesses be eliminated or adequately mitigated?**

No comment.

b. **Are Certificate Authorities subject to any form of oversight?**

i. **If so, by whom and how does this function?**

No comment.

ii. **If not, would enhanced oversight help address the weaknesses examined in Question 1? Why or why not?**

No comment.

c. **Are there alternatives to the digital certificate model?**

i. **If so, what are they?**

No comment.

ii. **If not, how can the current digital certificate ecosystem be improved?**

No comment.

10. **In your testimony, you discussed the attribution of threats, and how it is a function of "what is at stake."**

a. **What are the factors that influence the success of attribution, especially if a breach is not considered high-profile?**

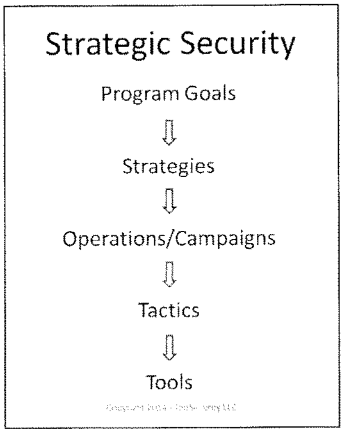
I strongly recommend reading "Attributing Cyber Attacks" (bit.ly/attributing-cyber-attacks) by Dr Thomas Rid and Ben Buchanan for the definitive scholarly article on attribution. In brief, from their paper:

"[A]ttribution is what states make of it. Matching an offender to an offence is an exercise in minimising uncertainty on several levels. On a technical level, attribution is an art as much as a science. There is no one recipe for correct attribution, no one methodology or flow-chart or check-list. Finding the right clues requires a disciplined focus on a set of detailed questions — but also the intuition of technically experienced operators. It requires coup d'œil, to use a well-established military term of art.

On an operational level, attribution is a nuanced process, not a simple problem. That process of attribution is not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades. As a result, it is also a team sport — successful attribution requires more skills and resources than any single mind can offer. Optimising outcomes requires careful management and organisational process.

On a strategic level, attribution is a function of what is at stake politically. The political stakes are determined by a range of factors, most importantly by the incurred damage. That damage can be financial, physical, or reputational. Viewed from the top, attribution is part resourcing and guiding the internal process; part participating in final assessments and decisions; and part communicating the outcome to third parties and the public."

b. How does attribution of the threat help a company or organization recover from a breach?



I will explain how attribution can assist responsible actors, from defenders through policymakers, using the diagram at left.

Starting from the bottom, at the Tools level, attribution matters because identifying an adversary may tell defenders what software they can expect to encounter during an intrusion or campaign. It's helpful to know if the adversary uses simple tools that traditional defenses can counter, or if they can write custom code and exploits to evade most any programmatic countermeasures.

Vendors and software engineers tend to focus on this level because they may need to code different defenses based on attacker tools.

The benefits of attribution are similar at the Tactics level. Tactics describes how an adversary acts within an engagement or "battle." It describes how the foe might use tools or techniques to accomplish a goal within an individual encounter.

For example, some intruders may abandon a system as soon as they detect the presence of an administrator or the pushback of a security team. Others might react differently by proliferating elsewhere, or fighting for control of a compromised asset.

Security and incident response teams tend to focus on this level because they have direct contact with the adversary on a daily basis. They must make defensive choices and prioritize security personnel attention in order to win engagements.

The level of Operations or Campaigns describes activities over long periods of time, from days to months, and perhaps years, over a wider theater of operations, from a department or network segment to an entire organization's environment.

Defenders who can perform attribution will better know their foe's longer-term patterns of behavior. Does the adversary prefer to conduct operations around holidays, or certain hours of the day or days of the week? Do they pause between tactical engagements, and for how long? Do they vary intrusion methods? Attribution helps defenders answer these and related questions, perhaps avoiding intrusion fatigue.

CISOs should focus on this level, and some advanced IR teams incorporate this tier into their work. This is also the level where outside law enforcement and intelligence teams organize their thinking, using terms like "intrusion sets." All of these groups are trying to cope with long-term engagement with the adversary, and must balance hiring, organization, training, and other factors over budget and business cycles.

At the level of Strategy, attribution matters to an organization's management and leadership, as well as policymakers. These individuals must decide if they should adjust how they conduct business, based on who is attacking and damaging them. Although they might direct technical responses, they are more likely to utilize other business methods to deal with problems. For example, strategic decisions could involve legal maneuvering, acquiring or invoking insurance, starting or stopping business lines, public relations, hiring and firing, partnerships and alliances, lobbying, and other moves.

Strategy is different from planning, because strategy is a dynamic discipline derived from recognizing the interplay with intelligent, adaptive foes. One cannot think strategically without recognizing and understanding the adversary.

Finally, the level of Policy, or "program goals" in the diagram, is the supreme goal of government officials and top organizational management, such as CEOs and their corporate boards. These individuals generally do not fixate on technical solutions. Policymakers can apply many government tools to problems, such as law enforcement, legislation, diplomacy, sanctions, and so forth. All of these require attribution. Policymakers may choose to fund programs to reduce vulnerabilities, which in some sense is an "attribution free" approach. However, addressing the threat in a comprehensive manner demands knowing the threat. Attribution is key to any policy decision where one expects other parties to act or react to one's own moves.

c. What makes attribution so difficult?

It is difficult because the amount of time and effort required to perform attribution is disproportionate to the amount of time and effort required to frustrate attribution.

11. We often hear about intrusions that effect consumer data but we don't often hear about the threats to Intellectual Property.

a. How prevalent are the threats to Intellectual Property?

I defer to the Commission on the Theft of American Intellectual Property (The IP Commission, www.ipcommission.org).

b. How does the economic impact of Intellectual Property theft compare to something like the theft of consumer data?

I defer to the Commission on the Theft of American Intellectual Property (The IP Commission, www.ipcommission.org).

c. Is it possible to quantify the economic effect of stolen Intellectual Property?

I defer to the Commission on the Theft of American Intellectual Property (The IP Commission, www.ipcommission.org).

d. Please describe the types of cyber threats to the U.S. economy (e.g. IP theft, theft of consumer data, etc.) and, to the extent possible, rank them in terms of severity of economic impact.

I defer to the Commission on the Theft of American Intellectual Property (The IP Commission, www.ipcommission.org).

12. You stated in your written testimony that the average breach goes undetected for nearly seven months, and that we have only gotten marginally better at identifying intrusions over the last three years (38 day reduction).

a. Why is it so challenging to identify these threats once they are in a system or network?

The majority of organizations do not conduct a security program with a goal of minimizing loss due to intrusion, with a strategy of rapid detection, response, and containment. Because they are not looking for intruders already present in the network, they end up learning about breaches when third parties notify them.

i. Are certain sectors better at identifying vulnerabilities than others?

In general, defense and finance companies operate the most mature private sector incident detection and response programs.

ii. Is there variation based on the size of the company? If so, why?

The larger the company, the more likely they will have a mature program. It is expensive to sustain security programs capable of frustrating a range of threat actors. Only the largest companies can afford to distribute the cost of the team across a large information technology or security budget.

b. Once a breach is identified, how difficult is it to remediate the threat?

i. Based on your experience, do you have a sense of how long, on average, this process takes?

It can be exceptionally difficult to dislodge an intruder, or groups of intruders, once they have been resident for weeks, months, or years. Depending on the nature of the threat and their dedication to retaining access, it may take weeks to remove them. However, if the threat actors receive tasking to return to the victim network, the organization will likely confront a long-term campaign.

c. **If it is so difficult and time consuming to identify and remove bad guys from a system, how can we ever expect to keep pace with the threats?**

The only strategy I have seen work during the 18 years of my career has relied on detecting and responding to intrusions before the adversary accomplishes his mission.

13. **In your testimony you described an equation that defines risk as the product of threat, vulnerability and cost. When any of those three factors increase, so does risk, and vice versa. You also described the pitfalls of focusing too heavily on any one factor, like vulnerability. We hear quite a bit about C-suite executives who worry primarily about the cost of security, and about Chief Information Officers and Chief Information Security Officers who worry primarily about vulnerabilities.**

a. **Do you believe that this mismatch of priorities is part of the reason why cybersecurity is such a difficult problem to approach?**

I believe, and many others concur, that cyber security is a "wicked problem" (en.wikipedia.org/wiki/Wicked_problem). Simson Garfinkel described it in these terms:

"There is no clear definition of the wicked problem. (You don't understand the problem until you have a solution.)

There is no "stopping rule." (The problem can never be solved.)

Solutions are not right or wrong. (Benefits to one player hurt another.)

Solutions are "one-shot." (No learning by trial and error. No two systems are the same. The game keeps changing.)

Every wicked problem is a symptom of another problem."

This description is derived from Garfinkel's 2012 presentation (www.afcea.org/events/tnlf/east12/documents/2012-04-25_Cybersecurity.pdf), which summarized an October 2011 Chatham House article by Dave Clemente, "Cyber Security as a Wicked Problem" (www.chathamhouse.org/publications/twt/archive/view/178579).

b. **How can executives and security professionals reconcile their different priorities and views?**

In my five levels of strategic thought -- goal, strategy, operations/campaigns, tactics and tools -- I see chief security officers (CSOs) as a bridge, usually working at the operational level, between the CXOs and board members and the security teams and vendors. I prefer to see CSOs speak policy and strategy to the CXOs and board members, and tactics and tools to the security teams and vendors, while running operations from the CSO office. This is a shift in mindset and approach, but I am seeing signs that it is welcome and effective.

The Honorable Markwayne Mullin

1. **I know you probably wouldn't naturally associate Oklahoma with advanced cybersecurity, but Oklahoma's Cyber Command Security Operations Center is considered one of the most advanced state security systems out there. Last week, I had a chance to speak with our Chief Security Officer, Mark Gower and Dr. Jerry Dawkins of True Digital Security, which is based out of Tulsa. One of the topics that came up in both of these conversations was how cyber threats are particularly harmful to small and medium-sized businesses. When my wife and I went into business 17 years ago, cybersecurity was pretty low on the list of things we worried about. Mr. Bejtlich, can you briefly speak to the challenges that a small or medium-sized business faces when it comes to cybersecurity that a large business might not have to deal with?**

Depending on the nature of the company, a SMB might face all of the challenges of a large business, but lack the resources to meet those challenges. The SMB will likely lack the resources because it cannot scale its expenses across a larger revenue base.

2. **What advice would you give to an entrepreneur opening up, say, a retail shop or restaurant?**

1. Identify and minimize information assets. Do you really need that data? This question prompts the user to consider whether the data they collect, store or transmit is truly necessary for business operations. Sometimes, outside regulators seek to control data, as is the case with the Payment Card Industry Data Security Standard (PCI DSS). Even when not regulated, everyone, from corporate employees to home users, should think about the sorts of data they manipulate. The best way to keep sensitive data out of the hands of criminals might be to never let it exist in digital form.

2. Keep sensitive data off the network as much as possible. Everyone has sensitive data, but not all that data needs to be connected to a network. For example, a company processing tax returns could keep that information on systems not connected to the Internet. Alternatively, sensitive data might reside on external hard drives that are attached to a PC or laptop when needed, and detached when not needed. If a criminal can't reach sensitive data because it is off the network, he can't read, steal, or delete it.

3. Provision a separate PC for sensitive business functions, like banking. SMBs should identify one or more computers to be used only for sensitive functions, like electronic commerce. The PC used to transfer money from one account to another should only serve that function. Users should not check their email, browse random Web sites, connect USB thumb drives, or take any other actions on the "e-banking PC." Criminals want to steal the usernames and passwords associated with bank accounts, but their job is a lot harder if users never check email or Web sites on the computer they use for doing banking. If possible, only connect this PC to the network when doing electronic commerce.

4. Enable two-factor authentication (2FA) wherever possible. 2FA refers to practices that require users to log into accounts using something more than a username and password. Some readers may be familiar with tokens that flash a new six-digit code every minute or so. Free solutions, like Google Authenticator are another option. Some sites provide users with the option of adding a code sent via Short Message Service (SMS) texts, sent to mobile phones. No solution is hack-proof, but whatever option a service provides above and beyond simple usernames and passwords, users should test and adopt.

5. Leverage trustworthy cloud solutions. Most computer users aren't interested in being information technology experts. Many SMBs can't afford in-house IT departments, or don't consider IT as a core

business function. In these cases, companies should evaluate cloud providers. Theoretically, a cloud provider can hire the necessary expertise to keep data secure, and scale that expertise across the customer base. The trick is identifying trustworthy cloud providers. Ask or research the following questions: 1) what government agencies subscribe to the cloud solution, and 2) what documentation can the cloud provider provide concerning its security practices? Cloud providers who fail these two tests may not yet be ready for conscientious SMB customers.

6. Join Infragard. Infragard is a non-profit organization run by the US Federal Bureau of Investigation. The FBI created Infragard in 1996 to assist the private sector with cyber defense. Infragard maintains chapters in virtually every major city across the country. These chapters hold regular meetings with content designed to educate attendees on cyber threats and mitigations. Such events allow attendees to learn from each other, and also meet their local FBI agents. Organizations should become acquainted with their respective law enforcement agents prior to any serious security incident. The worst time to first meet an FBI agent is when you need that agent's help with a computer intrusion.

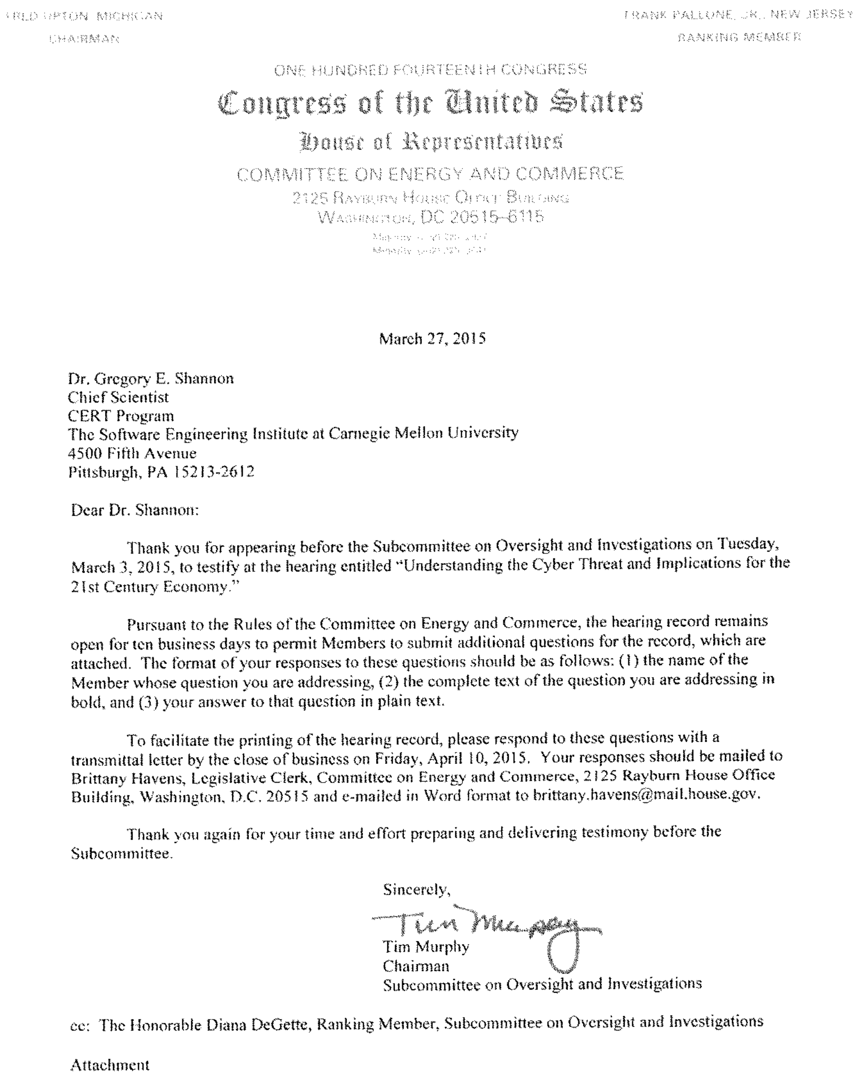
7. Treat cyber security as a business problem, not a technical problem. Business leaders have traditionally considered cyber security to be a problem for the IT staff. Executives thought that if they just bought the right software, they could "solve" the "hacker problem." However, the pervasiveness and consequences of digital breaches have encouraged those leaders to properly consider digital defense as a business problem. No one buys a software package to manage human resources, believing that the new application has "solved" hiring, retention, and other personnel challenges. No one subscribes to a cloud-based sales solution, thinking that they have "solved" their customer acquisition and satisfaction problems. In a similar way, executives will find security software to be necessary, but not sufficient, to address hacking woes. It is important for leaders to devise a security strategy appropriate for their business, then execute on that strategy on a daily basis.

3. **How can businesses be sure that their vendors understand their specific cybersecurity issues and will develop a system that will provide protection?**

Choose vendors with a reputation for caring about security. For example, is the vendor a member of the Forum of Incident Response and Security Teams (www.first.org/about/organization/teams)? Does the vendor operate a product security incident response team (PSIRT) or at least have a "/security page" on their Web site (e.g., www.fireeye.com/security), offering ways to contact the vendor about security issues? These are useful starting points.

4. **Would you say that security breaches we see in small businesses are an IT problem or a business problem?**

All security problems are first and foremost business problems.



FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 Rayburn House Office Building
Washington, DC 20515-6115
Majority [illegible]
Minority [illegible]

March 27, 2015

Dr. Gregory E. Shannon
Chief Scientist
CERT Program
The Software Engineering Institute at Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Dear Dr. Shannon:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, March 3, 2015, to testify at the hearing entitled "Understanding the Cyber Threat and Implications for the 21st Century Economy."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, April 10, 2015. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to brittany.havens@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Gregory E. Shannon, PhD, Chief Scientist

The CERT Division, Software Engineering Institute, Carnegie Mellon University

Questions for the Record:

Hearing on "Cyber Threats and Implications for the 21st Century Economy," before the Subcommittee on Oversight and Investigations, U.S. House of Representatives Committee on Energy and Commerce, held March 3, 2015

Attachment I-Additional Questions for the Record

The Honorable Tim Murphy

1. Each witness provided a slightly different perspective on cyber threats and the challenge of cybersecurity, extending from the past to the present and future.

a. *Are there areas where you feel there is a common view or shared theme and what is it?*

The continued success and growth in networked systems (aka, the Internet) drives the increases in cyber threats and risks. Design decisions made decades ago continue to reverberate in the cyber-security and privacy challenges we see today and will see as the Internet of Things unfolds in the next five to ten years.

Each entity (gov't, corporate, individual) must mindfully manage their cyber risks with efficient mitigations. And, many/most entities consistently fail at such mindfulness.

Gov't should consider how to best enable/encourage entities to be mindful about cyber risks and mitigations. Regulation often is a poor option since it usually encourages compliance rather than engaged consideration of risks.

b. *Ifthere was one fundamental message you want Congress and the public to understand about cybersecurity, what would it be?*

Mindfully manage cyber risks; demand mitigations that are more efficient.

c. *Are there specific issues or areas ofthis issue that do not receive an appropriate level ofattention?*

The need for research to be a part of the information sharing discussion. Not only do researchers need access to data to invent better tools, but we also need to include the sharing of vulnerability discoveries (before an attack) as well. Research is also needed to understand how to best digest shared information as well as what information is truly valuable/necessary to ingest.

Furthermore, research needs to be considered in major policy decisions – what is the evidence of likely efficacy for the policy? There are too many policies presented as "good ideas" or "the obvious/right thing to do" but are without supporting evidence that the policy would be followed or have the expected impact (often the desired impact isn't stated...).

2. As the promise of innovation connects more of our lives to cyberspace – from smart pacifiers to cars that communicate with each other -cyberspace becomes, in theory, a limitless attack surface.

a. *How do we manage the risks presented by "smart devices" and the Internet of Things while also enjoying the benefits and convenience they offer to society?*

Promote robust tool chains that automatically provide sound security and privacy without developer/programmer action. Encourage the development of such tool-chain ecosystems. The initial steps to improving this area would include defining and implementing a standard definition of "robust" across the relevant industries and standard ways to assess against this definition.

b. *As more devices connect to cyberspace and interact with one another, what challenges does this present for how security professionals or companies anticipate potential vulnerabilities or risks?*

Companies will be overwhelmed (and possibly fail as businesses) if they don't mindfully manage the relevant cyber risks. Better understanding of which risks to manage and how to prioritize risk, along with budget constraints, will continue to be a huge challenge. We will see the problem of complexity continue to evolve and become more important. Companies will find it difficult to know which systems, vulnerabilities, and threats are important to maintaining the resilience and safety of the IoT. This is not only because of the complexity of the systems themselves, but also because of the rapid pace with which supply chain relationships can change.

c. *How do we assess the security of individual products relative to the security of the system as a whole?*

Piloting new solutions in small scenarios and in situ, especially. By assessing the thoroughness and quality of the processes used to design, implement, and manage the risks of these products over time.

d. *In such an interconnected world, how do you draw the line between a potential vulnerability and a realistic vulnerability? In other words, just because something is possible, how important is it to assess the probability that it will occur?*

There are two aspects to assessing a vulnerability, both of which need to be periodically assessed since circumstances can change/evolve (sometimes quickly). (1) How are key assets affected by the vulnerability? Does this vulnerability enable a

path for an adversary (e.g., from HVAC controls to Point-of-sale terminals)?
(2) Are adversaries exploiting that vulnerability or have they shown interest in such the path enabled by the vulnerability?
Yes, the probability has to be weighted, though the more valuable the target the higher the probability. And, adversaries might know of or have imagined paths that the organization's security staff haven't considered.

3. Quite a few respected technologists -at Google, and also at the Institute of Electrical and Electronics Engineers Computing Society – have theorized that in the future, the Internet will be so integrated into our daily lives that it will become "invisible" and provide "seamless intelligence."

a. *Can you expand a little more on how exactly a world with an "invisible" Internet would work?*

It (the Internet) is everything in that everything is connected to it. So, just like electric motors used to be something you bought/used as a separate item (see 20th century Sears catalogues) they now are everywhere and you don't think about them. As the internet becomes more accessible to everyone and more of our lives/things are connected to the internet, it will become invisible only in that we simply won't notice it anymore, much like you barely think about the ability to make a phone call from wherever you are.

b. *Do you agree with these predictions? Why or why not?*

I agree that "seamless intelligence" is what we'll expect and experience. However, it'll take decades for the Internet to become "invisible," especially because we/society will struggle with new and old security and privacy challenges as the particulars of these technologies evolve. And, there will be failures, some painful, hopefully none catastrophic.

4. No matter how much money a company invests in security software, training and other cybersecurity measures, they still remain vulnerable to the insider threat. This can range from the intentional actor –such as a disgruntled employee stealing information or letting the bad guys in-to inadvertent actors-such as an employee clicking an infected link in a targeted phishing email.

a. *Will companies ever be able to prevent internal threats-employees lowering the proverbial draw bridge-regardless of whether their actions are intentional or unintentional?*

Companies can certainly mindfully mitigate insider threats. But no, they won't be able to prevent/eliminate them.
No matter how much money a company invests in security software, training, and other cybersecurity measures, they still remain vulnerable to the insider threat due to the fact that trusted insiders are needed for an organization to achieve its mission and to do so, need to be granted authorized access to critical assets. While this is true, it does not mean that an organization is unable to take steps to reduce the likelihood that an insider could cause harm. Many recent high-profile incidents were caused by an insider who intended to cause harm, whether that be an

individual who: stole information from an organization; stole money or defrauded an organization; sabotaged the organization; or disclosed classified information causing harm to the United States. Malicious insiders should be a threat recognized by an organization when building its protection strategies but also they must recognize the threat posed by non-malicious insiders who could cause harm, without intent.

b. *If it can never be eliminated, does it come down to managing risk? Are there proven strategies to minimize this risk?*

Yes and yes. Insiders, including current employees, contractors, and other trusted business partners, to whom an organization grants authorized access to its critical assets, including its facilities, people, technology, and information, do have the ability to harm the organization, but the vast majority do not pose a significant threat because most lack the access and the motivation to cause harm. It is a widely accepted security best practice to limit authorized access to the minimum number of assets necessary for someone to do his job. By doing so, an individual does not pose a threat to everything in the organization. An organization should consider identifying and protecting its critical assets from all threats, both external and internal, with the internal threats being posed by only those with authorized access. By monitoring the asset, anomalies of access and modification can be alerted, triaged, and investigated. But not all insiders are a threat.

To protect against the unintentional insider harming the organization, a combination of technical and administrative controls should be implemented in addition to requiring regular security awareness training. Training should focus on making insiders aware of their responsibility in protecting the organization's assets, including specific techniques, tactics, and procedures used by adversaries to gain access into the organization, allowing potential compromise of its assets. Employees should be made aware of the fact that they can be a target and that targeted social engineering attempts may be made possible because of the information they make publically available.

Carnegie Mellon University's Software Engineering Institute offers multiple options for training and implementing Insider Threat programs in organizations. These programs prepare organizations to meet the intent of Executive Order 13587 -- Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. More information on the various programs can be found at https://www.cert.org/training/ and is available in multiple publications including the Addison-Wesley book, *The CERT Guide to Insider Threats,* and *The Common Sense Guide to Mitigating Insider Threats.*[1]

The lack of validated, efficient mitigations is a significant challenge. However, researchers are looking at mitigation strategies (organizational and technical) that have other benefits to organizations. For example, well-engaged staff very rarely are insider threats (even unintentional threats) due to their dedication to and mindfulness of their organization's mission. So, efforts to increase employee engagement with their work are expected to decrease insider threats from those employees.

[1] Common Sense Guide to Mitigating Insider Threats is found here: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

c. *How significant of a challenge is this to those evaluating the cost benefit of security measures?*

Organizations must recognize the significant challenge when attempting to calculate and evaluate the cost benefit of security measures. Most organizations are limited by resource constraints, including limited time, people, and money to implement the optimal security solution. In addition, security implementations, if implemented at too high of a level, approaching a 100% solution, may prohibit an organization from achieving its mission. Organizations should strive to implement a solution that protects its assets to the greatest practical extent; identify and choose to accept the risk of implementing less than the optimal solution; and protect the organization from threats that originate from outside and inside the organization, including both those that are malicious and non-malicious.

5. Information sharing, though it has its benefits, is still a reactionary solution. Someone has to first suffer an attack before that threat information can be shared, and oftentimes the attackers change their signatures from target to target.

a. *How does information sharing help reduce the gap between cybersecurity capabilities and threats to cybersecurity described in Dr. Lin's testimony?*

Sharing information lets defenders know the current active threat vectors, especially if some threat is active "at scale". However the gap is only reduced if those receiving the information first understand it and second, know how to effectively take action – which is often not the case. Companies that have high levels of cyber security tend to already be aware of the threat, those who are unaware are also the ones who lack the institutional knowledge (or budget) to do anything about it anyway. So a large and detrimental gap exists in terms of cyber skills and budget that information sharing does not fix.

b. *There is a lot of focus on signatures when it comes to information sharing.*

i. *Are signature-based defenses effective? Why or why not?*

Yes and no.

Yes, they're easy; there are commercial products that support such approaches, and security staff have training on how to use them.

No, savvy adversaries know how to thwart signature-based defenses.

c. *How does information sharing fit into the broad picture of the cybersecurity challenge?*

It's a community response, which is important in order to make everyone feel like they own at least part of the problem and the solution.

Information sharing is one way defenders can accelerate dynamic response to threats – in minutes/hours vs. today's days/months.

While important, it does not truly fix much, considering the vulnerability is the weakest link – a point of entry that would not know what to do with such information even if they had it.

i. *Does it offer opportunity beyond improving our defensive capabilities?*

Yes, if we can correlate reports with organizational behaviors. We're just starting to see some studies on such data, but that work is typically done by private organizations with special access to a small amount of data.

It can if we allow the research community access to information – to allow for better innovation and cyber security solutions. If we included vulnerability disclosure (the discovery of a vulnerability *before* it is exploited) into the discussion, then that would greatly improve the landscape.

6. Is it possible to quantify the benefits of the Internet and information technology relative to the cost of security?

a. In other words, is it possible to calculate the economic benefits of these technologies relative to the economic costs of cybersecurity, including prevention and response in the event of a breach?

Not easily.

At the micro level it's very difficult given the lack of data to measure the collectively experienced impact of security practices. However, it is possible for an organization to calculate the economic benefits of using technology versus the risks that it poses to the organization. We (CERT) are working on a model that takes into account the impact of a cybersecurity event on the outcomes of the organization's mission. Using this model results in a dollar amount, or cost, of the impact. This amount can then be compared to the cost of the technology that could detect, protect, respond to, and/or recover from the event.

At the macro level the State Department is looking at this (The Office of the Chief Economist), and I've seen an interesting presentation by Mellissa Hathaway on how cybersecurity investments appear to impact GDP (in an October 2014 talk for OAS titled Lessons Learned in the Design of National Cyber Security Strategies, http://www.iadb.org/en/news/news-releases/2014-10-22/cybersecurity-workshop-for-latin-america,10957.html).

b. How about the social, cultural or other less tangible benefits?

Yes, it is possible to calculate the cost of less tangible benefits. These calculations may be organization- or sector-specific, but they can and should be included as part of the overall cost benefit model. As one example, an enterprise risk management program should include determinants of, quantification of, and ways to manage reputational risk when appropriate to an organization.

c. Is there value in this?

Absolutely. There is not only value in doing this, but it is critical for some organizations to include these as part of effective risk management programs. While the actual values and categories will differ between organizations, the process for building and implementing a risk management program should include weighted values to compare the benefits of cybersecurity capabilities against the cost.

Cybersecurity and privacy involve significant positive and negative externalities, which are part and parcel of policymaking. We continue to improve our understanding of these dynamics, especially as more and more critical infrastructure is (overly?) connected to the Internet.

7. Discussions about cybersecurity often focus on prevention or keeping actors out of system -Is this the right way to approach this issue?

a. *If there is no guarantee the bad guys won't get in, should the emphasis shift to a focus on resilience rather than prevention?*

The emphasis should shift to a focus on resilience – and prevention is but one piece of a resilience program. Given the current state of IT technologies, you have to assume adversaries can/will get in, or are in, your systems.

Resilience encompasses identifying the most critical assets to an organization's mission – these assets can be people, information, facilities, or technology. Once the critical assets are identified, there should be a balanced approach across protection, detection, response, and recovery so that an organization can continue to provide service or meet its mission DESPITE the disruption or cybersecurity event.

So, (1) we need to work to efficiently make "getting in" more difficult and (2) ensure that once "in" it is difficult to significantly disrupt operations. Unfortunately, we have limited efficient mechanisms for either – R&D is needed both by government and the private sector.

b. *Why is the concept of resilience important to effective cybersecurity?*

Resilience is important because we cannot control the ever-changing and evolving threat landscape, but we can control our actions to protect, detect, respond to, and recover from incidents. Resilience is going to be the basis of economic and social survival – we need to avoid fragility and brittleness under "failure" --we must be able to recover. Resilience takes into account events, incidents, and threats not intended to disrupt technology, but the important things connected to technology. This includes not only failures in technology itself, but also the actions of people, failures in process, and even natural disasters that can disrupt organizations. Approaching cybersecurity as another potential operational risk provides better potential to incorporate practices into the organization's risk management process as a means to resilient operations. In recognition of the need to shift to resilience, CERT developed the CERT-Resilience Management Model (CERT-RMM)[2] as a foundation for a process improvement approach to operational resilience management. CERT-RMM is a maturity model that defines the essential organizational practices that are necessary to manage operational resilience. An organization can use CERT-RMM to determine its capability to manage resilience, set goals and targets, and develop plans to close identified gaps. By using a process

[2] http://www.cert.org/resilience/products-services/cert-rmm/

view, CERT-RMM can help an organization respond to stress with mature and predictable performance. Actively used derivatives of CERT-RMM include the Department of Homeland Security's Critical Resilience Review (CRR), used for assessing an organizations cybersecurity practices in ten select domains of practice.

c. *How does resilience support a risk-based approach to cybersecurity?*

Resilience is an advanced form of risk management. Resilience not only takes into account the risks, but it focuses on the impact to the critical few assets so that limited resources can be applied to ensure that an organization can still meet its mission even through disruption. Resilience management enables organizations to transform uncertainties into measurable operational risks and then to efficiently manage those risks while maintaining operations.

d. *In your written testimony, you mentioned the Cybersecurity Capability Maturity Model (C2M2) in your submitted testimony. Can you expand upon this program and how if differs from other options, such as the NIST Framework?*

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[3] is a joint Department of Energy (DOE) and Department of Homeland Security (DHS) effort to help energy sector organizations determine their cybersecurity posture. The ES-C2M2 comprises a maturity model, an evaluation tool, and voluntary DOE facilitated self-evaluations. The model is a collection of cybersecurity practices grouped in ten domains and arranged according to maturity levels. Measures of performance are applied to each domain. The evaluation tool allows an organization to compare its security practices against the criteria of the ES-C2M model. These scores can be compared to target levels of performance to determine gaps in cybersecurity capabilities.

The ES-C2M2 was preceded by the DHS Cyber Resilience Review (CRR).[4] The CRR also measures cybersecurity posture by means of a capability maturity model (CERT-Resilience Management Model[5]), an automated self-assessment evaluation tool, and voluntary DHS facilitated evaluations. The CRR was designed to be applicable to all critical infrastructure sectors, and does not contain the sector-specific tailoring of the ES-C2M2. The CRR also examines the maturity of cybersecurity practices organized into ten distinct domains. In both the ES-C2M2 and the CRR maturity is defined as the institutionalization of cybersecurity practices and processes. Institutionalized practices and processes are more likely to continue to operate effectively during a time of organizational stress (e.g. cyberattack). This examination of maturity differentiates the ES-C2M2 and CRR from more traditional assessments of cybersecurity in which conformance to a standard practice is the only element being measured (e.g. NIST 800-53, ISO/IEC 27001:2013, etc.).

The NIST Framework for Improving Critical Infrastructure Cybersecurity, more

[3] http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

[4] https://www.us-cert.gov/ccubedvp/self-service-crr

[5] http://www.cert.org/resilience/products-services/cert-rmm/

commonly known as the NIST Cybersecurity Framework (NIST CSF),[6] arranges cybersecurity practices into a of hierarchy of Functions, Categories, and Subcategories. Categories are analogous to the domains of the ES-C2M2 and the CRR. Subcategories are roughly equivalent to the specific practices contained within the domains of the ES-C2M2 and CRR. The NIST CSF is not a maturity model and does not evaluate the institutionalization of practices and processes. The completeness of prescribed practices is the exclusive focus of the NIST CSF. The framework does apply a progression of Implementation Tiers to measure the integration of cybersecurity risk management activities. These should not be confused for the measures of process maturity found in the ES-C2M2 and CRR. Using the NIST CSF does not preclude an organization from also applying the ES-C2M2 and CRR. The evaluation methods can be used in combination. Both the ES-C2M2 and CRR assessment packages include detailed correlation of results to the criteria of the NIST CSF, so an organization can use those assessments to determine if it has met the criteria of the NIST CSF.

8. In Dr. Lin's written testimony he stated that "complexity is the enemy of cybersecurity."

a. *Do you agree with this assessment?*

Yes, given the way cybersecurity is practiced today, complexity does make cybersecurity harder, more expensive, and less effective.
However, I believe that complexity here is more about a lack of understanding about what systems can/should/could do and how adversaries might breach them.

b. *Is it possible to reduce this complexity?*

Yes, by creating technical ecosystems that have security and privacy properties built in (e.g. to tool chains) so that only a few specialists need to fully appreciate the security challenges and have the tools and knowledge to ensure that whole ecosystem is protected. If we can do this, then our adversaries will have to work much harder to disrupt cyberspace.

i. *If yes, what are the consequences?*

ii. *If no, why not?*

9. **In the last few years, there have been several significant compromises and vulnerabilities discovered in regards to digital certificates and Certificate Authorities two of the best well known being the compromise of DigiNotar and the recent Lenovo/Superfish revelations. This raises questions as to whether the digital certificate model is providing an adequate level of security for users of the Internet.**

Note: CERT is organizing a workshop for this summer on operational security challenges and opportunities for the global PKI, especially certificate authorities.

a. *What are the weaknesses in the digital certificate model?*

There are no proofs of correctness for the software that implements these protocols and there's been limited formal analysis of the protocols as used in practice. Hence,

[6] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

adversaries can readily discover and exploit gaps.

When it comes to authentication and encryption, there are weaknesses with the current PKI model used by SSL. When validating SSL, the trust anchor lies in each certificate authority (CA). There are a few things to keep in mind:

- Your browser or OS chooses the "trusted" CAs, not you.
- Any CA may issue a certificate for any domain.
- The weakest CA determines the strength of the whole PKI.

http://www.net.in.tum.de/fileadmin/bibtex/publications/papers/ssl-landscape-trento.pdf

There are currently more than 100 trusted CAs across modern platforms. For the PKI architecture to work, each one of these CAs must provide due diligence to:

1. Not get hacked (DigiNotar, Comodo)
2. Not get tricked
3. Follow the Certification Practice Statement (CPS) policy that they have published
4. The CPS (and any other certificate issuance and verification processes) must be sound

http://googleonlinesecurity.blogspot.com/2015/03/maintaining-digital-certificate-security.html

PKI centers around the use of trusted third parties. As it is currently implemented, Internet-scale PKI requires trust in all 100+ Certificate Authorities, with little defense should one or more be untrustworthy whether due to error, sloppy business practices, or malice.

When a user visits a site over HTTPS and their browser does not indicate a certificate problem (i.e., when it all works), at best that means that the certificate received was issued by one of the root CAs that is trusted by the browser. Due to the point-to-point nature of SSL and its associated PKI architecture:

- End-to-end encryption is **not** guaranteed.
- End-to-end authentication is **not** guaranteed.

i. *How significant are these weaknesses?*

Significant. Certifications are the foundation of trust transmission on the Internet.

Each of the requirements of CAs outlined above have been violated at some point. That is, CAs have been hacked, tricked, and been found to violate their own CPS policies. The result of these incidents is that users' expectations of encryption and authentication are violated. Traffic that should be protected by SSL could be spoofed, monitored, or altered by an attacker.

ii. *Can these weaknesses be eliminated or adequately mitigated?*

Yes, but it will take a sustained technical R&D investment as the weakness are numerous.

In its current form, the SSL PKI has an architectural design that prevents the weaknesses from being eliminated. There are some things that can help, though (see below).

b. *Are Certificate Authorities subject to any form of oversight?*

For the most part, no. There is some market pressure from web browser and operating system vendors who require CAs to meet certain standards in order to be included in browsers and operating systems.

i. *If so, by whom and how does this function?*

Software vendors that include the Certificate Authorities in the trusted root CA stores of their respective software are currently the primary oversight. For example, if a CA violates the policy that Mozilla holds them to, then Mozilla can choose to remove the trust in that CA (https://groups.google.com/forum/m/#!msg/mozilla.dev.security.policy/czwlDNbwHXM/amxjB32uY8AJ). Other software vendors such as Apple, Microsoft, and Google have the same control over the certificates that are included in their own trusted CA list. The CA/Browser Forum (https://cabforum.org/) is an organization that provides guidelines that CAs may choose to follow. However, participation in this consortium is strictly voluntary.

ii. *If not, would enhanced oversight help address the weaknesses examined in Question 1? Why or why not?*

It is likely that enhanced oversight would improve both the operation of the certificate authorities, as well as the public trust in them. The nature of the oversight matters though. Possibly variants of oversight include:

- standards for CAs

(The CA/Browser forum already has Baseline Requirements: https://cabforum.org/baseline-requirements-documents/)

- penalties for CAs that act negligently

(The FTC fined Kredit Karma and Fandago for claiming to use SSL to secure customer data but not verifying server certificates: https://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers)

- audit requirements to demonstrate compliance

Note that many nation-states either directly operate or exert significant influence over trusted Certificate Authorities, which broadens the range of threats that must be considered in determining appropriate oversight.

c. *Are there alternatives to the digital certificate model?*

Yes.

i. *If so, what are they?*

A "web of trust" model like OpenPGP uses is an alternative to the PKI infrastructure used by SSL and TLS. The Monkeysphere project is an example implementation of such a model. It is important to note that a critical mass of adoption must be achieved for a web of trust model to be viable, and this does not appear to have happened with the MonkeySphere project.

Another model is Trust On First Use (TOFU).

Other models integrate somewhat with existing PKI see the following question.

ii. *If not, how can the current digital certificate ecosystem be improved?*

From a technical perspective, there have been some attempts to layer additional checks on top of the underlying SSL PKI, such as the Convergence and Perspectives projects. However, neither of these projects appear to have attained the proper support for widespread adoption and success.

Certificate Transparency (http://www.certificate-transparency.org/) provides an open, public framework that can detect mistakenly issued or maliciously acquired certificates issued by a certificate authority. It can also help discovery of certificate authorities behaving badly (i.e., maliciously issuing certificates). Certificate Transparency is backed by Google and is being developed further in the IETF Public Notary Transparency (trans) working group (http://datatracker.ietf.org/wg/trans/charter/) At present, Certificate Transparency appears to hold the most promise for improvement in the near term.

From an operational perspective, increased transparency with respect to what happens within certificate authorities can help improve the current ecosystem. Given the number of CAs that various software platforms trust, it is currently difficult, if not impossible, for an end user to assign a level of trust to the SSL PKI in general. While some organizations that provide CA capabilities may be trusted by the user, there are a lot of "unknown" CAs that users have likely never heard of and have no ability to judge whether they are performing their due diligence to protect the user's security.

Using DNS (may require DNSSec, which is not widely available)

- http://tools.ietf.org/html/draft-hallambaker-donotissue-02
- https://datatracker.ietf.org/wg/dane/charter/

Certificate Pinning, Google

- https://www.imperialviolet.org/2011/05/04/pinning.html
- https://www.chromium.org/hsts/
- https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21

Google Certificate Catalog (--> Certificate Transparency?)

- http://googleonlinesecurity.blogspot.com/2011/04/improving-ssl-certificate-security.html
- http://www.certificate-transparency.org/

TACK

- http://arstechnica.com/security/2012/05/ssl-fix-flags-forged-certificates-before-theyre-accepted-by-browsers/
- http://tack.io/draft.html

Mutually Endorsing CA Infrastructure (MECAI)

- http://arstechnica.com/business/2012/02/ssl-fix-aims-to-mend-huge-cracks-in-nets-foundation-of-trust/
- https://kuix.de/mecai/mecai-proposal-v2.pdf

convergence/perspectives/observatory

- http://convergence.io/
- http://perspectives-project.org/
- https://www.eff.org/observatory

CERT is planning a workshop to discuss PKI issues, with potential DHS and IEEE support

10. In your written testimony you stated that we currently "'do not know" how to stop all serious cyberattacks while at the same time allowing for the efficient function of electronic commerce.

a. *Why don't we know? Is it that we currently do not have the technological expertise, or that technology has yet to evolve to a mature enough state?*

Both. Efficiency is the key. We know in theory how to make things secure, but the cover/overhead/usability is high, in some cases by many orders of magnitude.

b. *If the cause is that we do not currently have the technological expertise, how do we developsuchexpertise?*
More research, more training. Expansion of programs like scholarship for services.

c. *If the cause is that the technology is hot yet mature enough, what are the steps we need to take to accelerate that maturity?*

Access to operational data for researchers and measured pilot projects for developers/vendors.

11. In your written testimony you describe the need for "meaningful feedback" for what works if we are to encourage adoption of more effective safeguards or systems of security.

a. *Can you elaborate on what you mean by meaningful feedback?*

Does a practice or technology actually produce or correlate with operational security outcomes (e.g., fewer incidents). Individual organizations usually aren't large enough to measure such effects, but the gov't is if they can collect the data from sectors or nation wide.

b. *Can you give an example of how effective feedback could work in the real world for a small or medium business, given all the complexities and offerings in the marketplace?*

Yes. How much cyber-risk-management training is needed for a key staff member to efficiently mitigate common cyber threats at a Small and medium size businesses (SMB)? 1 Hour? 1 day? 1 week? 1 month? 1 year? Who should it be? If we could correlate the training practices of SMBs with their incident rates, that would then inform owners about what's an efficient investment – instead of just ignoring the problem wholesale. And, maybe the data shows that's there no efficient strategy other than ignore the problem – thought I doubt that.

c. *What progress has been made for developing a source of reliable information and measures of effectiveness?*

Limited. Though the NIST cyber risk management framework does offer hope.

d. *Is developing measures of effectiveness even possible in certain areas of cyberspace, given the size and complexities the networks?*

Absolutely yes. The focus has to be on outcomes, not behaviors or compliance. The question isn't "do we patch?", rather the question is "does patching reduce intrusions?" Also, since the adversary is adaptive, what works today might not work next year, so the outcome-based measurement of efficacy has to be continuous – this is one of the real efficiency opportunities for information/incident sharing.

12. In your written testimony you describe the need for medium-term solutions involving "richer data" to improve "situational awareness."

a. *What are the challenges to developing a better sense of situational awareness?*

Currently, access to data – and the privacy and liability concerns that accompany that.

Also, the tools and models to digest the data and present at a cognitively comprehensible view of the situation. A key situational awareness question is, who is trying to make what decisions? Research is continuing in this area. Too often "pretty visualizations" are seen as the answer without considering the decisions to be made.

b. *How does improved situational awareness affect the cost of cyberspace safeguards and security practices?*

With better situational awareness, less data would not only need to be shared – improving cost, but in theory solutions and tools could arise that allow for quick pinpointing of vulnerabilities and attacks, which would save time and money just in network flow analysis, forensics and response. Subsequently, if response is sooner damage is mitigated.

c. *As improvements in awareness occur in some portions of cyberspace, how do we translate that to prevent development of new vulnerabilities as cyberspace technologies expand?*

By seeing where adversaries continue to find success, vendors and customers can mindfully and more efficiently respond to systemic issues such as tools chains that produce vulnerable systems.

13. In your discussion of long term needs included in your written testimony, you note that there is no "silver bullet" but there are opportunities to increase the amount of energy required red for successful attacks.

This topic is the focus of my current technical research, so the answers are evolving, especially for non-technologists. I'll keep the committee staff informed of my progress.

a. *Can you please expand on what you mean by "energy based" barriers to cyber attacks?*

The goal is to create cyber infrastructure which requires an adversary to use a great deal of computing power (primarily electricity for the computers) to thwart/break a defense and cause a problem at scale (e.g., to the economy).

b. *What would be an example that a layman could understand?*

Encryption is already one example of a technology that we all use every day. Direct attacks on encrypted data are very expensive. This is known as "breaking the key." Only with lots of mega-watt years can you break most keys. Typically, the more long-lasting and central a key is, the key is designed to be hard to break.

c. *From your perspective, what progress is being made on this front and where is it most likely to develop -defense programs, private innovation?*

The ESCAPE workshop in June at CMU is meant to consider our technical progress (http://dimacs.rutgers.edu/Workshops/ESCAPE/announcement.html).

We're seeing progress both privately and with government research investments. There are multiple DARPA and IARPA programs addressing this challenge. And industry is starting to incorporate some of these technologies into their products, services, and business models.

d. *What in your view is the potential for the United States to achieve breakthroughs on this front, versus other nations?*

Very high. (1) we're willing to acknowledge the challenge and make investments.
(2) we have the R&D base to address the challenge.
(3) we can operationalize results through the highly-innovative parts of the software industry that are still predominately located in the US.

This can/should be an allied effort, though it's important the U.S. lead the way.

14. In your testimony, you talked about repositories of "pre-hardened" components such as programming libraries. Specifically, you said that such repositories would allow developers to access componen ts that have been tested and approved, therefore increasing the security and quality of the technologies they design.

Pre-hardening components is an idea that some of my fellow technologists have recommend. However, in my testimony, I was suggesting something (1) more general, (2) more easily adopted, and (3) that could facilitate such hardened repositories. In particular, I'm suggesting tool-chains (software frameworks, application programing interfaces (APIs), compilers, debuggers, editors, verification tools, etc.) that software engineers would use to create the artifacts (binaries) that one actually uses (executes) on a computer. We're already seeing this approach in frameworks, where security experts ensure that non-security engineers will create "safe(r)" artifacts. Those artifacts might be part of a library or it might be the actual application. These tool chains need not be regulated. An alternative approach is for the security evidence to be transparent in that how a tool chain assures a property is well documented, maybe even provable (in a mathematical sense).

One of the challenges with code repositories specifically is that they seem very similar to "code re-use" ideas promoted in decades past. Those "re-use" efforts often failed because of poor governance or business models. Hopefully, we have learned from "re-use" successes and failures.

a. *How would such a repository be created?*

These tool chains can be privately held by individual vendors, consortia, the government, as open source, etc. The governance of the tool chain and any repository is orthogonal to the technical security capabilities that it provides. A useful first public experiment might be SSL and PKI libraries and development tools since public key certificates are the foundation of security on the commercial Internet.

b. *What organizations, both public and private, would need to be involved?*

Public: NSF, NIST, DHS S&T, NSA-R, ASD(R&E)
Private: IEEE, ACM, ANSI, probably ISOC/IAB/IETF
Commercial: Key infrastructure providers willing to directly facilitate the approach

i. *Who would be responsible for such a repository?*

An existing or new non-profit, at least for the first steps.
Ideally open-source. A governance model (new or existing) would have to be worked out.

c. *Would a repository such as this be expensive to create and manage?*

i. *If so, how could those costs be managed?*

Initially as a community experiment; government could provide some funds/incentives, but involvement is voluntary.

d. *Who would be responsible for testing and approving the components that are made available through the repository?*

i. *Does such a repository raise liability concerns, if a "tested and approved" component is later found to be deficient?*

The model should be "tested with verifiable evidence reported", that way no new liabilities are created for participants. The liability onus could remain on the vendors who incorporate the software into their products.

ii. *If so, how could the repositories address and account for that liability?*

Depends on the governance, and actions gov't(s) could take.

e. *How exactly would developers use this repository?*

Download the artifacts and the accompanying tool chains and proceed in the context of their organization's development practices.

The Honorable Markwayne Mullin

1. It seems like whenever we start talking about the challenges that come with responding to any emerging industry or emerging threat, the issue of workforce development is front and center. With something like the engineering industry, we know we need to engage more students in STEM education, should we be treating the IT industry in the same way?

Yes, thought I thought we were (STEM and IT both are about technology, yes?).

IT is clearly a core enabling capability for operationalizing "STEM" innovations.
One challenge is that IT workers often have low status in their organization.
By raising the recognition of and respect for such workers, more students might see it as a rewarding occupation. Organizations need to highlight when IT staff have facilitated gains in productivity (and profits).